



Preface

This documentation describes how to use the Device Manager to configure the Cisco ACE 4700 Series Application Control Engine Appliance.

This section provides the following topics about the documentation:

- [Audience, page i](#)
- [Organization, page i](#)
- [Related Documentation, page iii](#)
- [Conventions, page v](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page v](#)
- [Open-Source Software Included in Cisco ACE Application Control Engine, page vi](#)
- [Open Source License Acknowledgements, page vi](#)

Audience

This documentation is intended for experienced system and network administrators. Depending on the configuration required, readers should have specific knowledge in the following areas:

- Networking and data communications
- Network security
- Router configuration

Organization

This documentation contains the following sections:

- [Chapter 1, “Overview”](#) contains an summary of ACE features and the ACE Appliance Device Manager interface, terms, and getting started configuration information.
- [Chapter 2, “Using Homepage”](#) describes how to use the DM Homepage, a launching point for quick access to selected areas within the DM.
- [Chapter 3, “Using DM Guided Setup”](#) describes how to use the guided setup pages to simplify configuration of the DM.

- [Chapter 4, “Configuring Virtual Contexts”](#) describes how to configure virtual contexts on the ACE appliance so that you can effectively and efficiently manage and allocate resources, users, and services.
- [Chapter 5, “Configuring Virtual Servers”](#) contains procedures for configuring virtual servers for load balancing on the ACE.
- [Chapter 6, “Configuring Real Servers and Server Farms”](#) provides an overview of server load balancing and procedures for configuring real servers and server farms for load balancing on the ACE.
- [Chapter 7, “Configuring Stickiness”](#) provides information about sticky behavior and procedures for configuring stickiness with the ANM.
- [Chapter 8, “Configuring Parameter Maps”](#) describes how to configure parameter maps so that the ACE can perform actions on incoming traffic based on certain criteria, such as protocol or connection attributes.
- [Chapter 9, “Configuring SSL”](#) describes the SSL configuration process and details the procedures for configuring SSL on the ACE appliance.
- [Chapter 10, “Configuring Network Access”](#) includes information about configuring virtual context VLAN interfaces, port channel interfaces, and Gigabit Ethernet interfaces.
- [Chapter 11, “Configuring High Availability”](#) contains an overview of the redundancy feature and explains how to configure high available.
- [Chapter 12, “Configuring Traffic Policies”](#) describes how to configure class maps and policy maps to provide a global level of classification for filtering traffic received by or passing through the ACE appliance.
- [Chapter 13, “Configuring Application Acceleration and Optimization”](#) describes how to configure application acceleration and optimization options on the ACE appliance.
- [Chapter 14, “Monitoring Your Network”](#) allows you to monitor key areas of system usage.
- [Chapter 15, “Managing the ACE Appliance”](#) describes the administrative tools that manage the ACE appliance.
- [Chapter 16, “Using ACE Appliance Device Manager Troubleshooting Tools”](#) describes the administrator-only diagnostic tools to help troubleshoot ACE appliance management problems.

Related Documentation

In addition to this documentation, the ACE appliance documentation set includes the following:

Document Title	Description
<i>Administration Guide, Cisco ACE Application Control Engine</i>	Describes how to perform the following administration tasks on the ACE: <ul style="list-style-type: none"> • Setting up the ACE • Establishing remote access • Managing software licenses • Configuring class maps and policy maps • Managing the ACE software • Configuring SNMP • Configuring redundancy • Configuring the XML interface • Upgrading the ACE software
<i>Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance</i>	Describes how to configure the web optimization features of the ACE appliance. This guide also provides an overview and description of those features.
Cisco Application Control Engine (ACE) Configuration Examples Wiki	Provides examples of common configurations for load balancing, security, SSL, routing and bridging, virtualization, and so on.
Cisco Application Control Engine (ACE) Troubleshooting Wiki	Describes the procedures and methodology in wiki format to troubleshoot the most common problems that you may encounter during the operation of your ACE.
<i>Command Reference, Cisco ACE Application Control Engine</i>	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
<i>CSS-to-ACE Conversion Tool Guide, Cisco ACE Application Control Engine</i>	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running-configuration or startup-configuration files to the ACE.
<i>Hardware Installation Guide, Cisco ACE 4710 Application Control Engine Appliance</i>	Provides information for installing the ACE appliance.
<i>Quick Start Guide, Cisco ACE 4700 Series Application Control Engine Appliance</i>	Describes how to use the ACE appliance Device Manager GUI and CLI to perform the initial setup and VIP load-balancing configuration tasks.
<i>Regulatory Compliance and Safety Information, Cisco ACE 4710 Application Control Engine Appliance</i>	Regulatory compliance and safety information for the ACE appliance.

Document Title	Description
<i>Release Note, Cisco ACE 4700 Series Application Control Engine Appliance</i>	Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE appliance.
<i>Routing and Bridging Guide, Cisco ACE Application Control Engine</i>	Describes how to perform the following routing and bridging tasks on the ACE: <ul style="list-style-type: none"> • (ACE appliance only) Configuring Ethernet ports • Configuring VLAN interfaces • Configuring routing • Configuring bridging • Configuring Dynamic Host Configuration Protocol (DHCP)
<i>Security Guide, Cisco ACE Application Control Engine</i>	Describes how to perform the following ACE security configuration tasks: <ul style="list-style-type: none"> • Security access control lists (ACLs) • User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network Address Translation (NAT)
<i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i>	Describes how to configure the following server load-balancing features on the ACE: <ul style="list-style-type: none"> • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • Dynamic workload scaling (DWS) • Firewall load balancing • TCL scripts
<i>SSL Guide, Cisco ACE Application Control Engine</i>	Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE: <ul style="list-style-type: none"> • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
<i>System Message Guide, Cisco ACE Application Control Engine</i>	Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.

Document Title	Description
<i>User Guide, Cisco Application Networking Manager</i>	Describes how to use Cisco Application Networking Manager (ANM), a networking management application for monitoring and configuring network devices, including the ACE.
<i>Virtualization Guide, Cisco ACE Application Control Engine</i>	Describes how to operate your ACE in a single context or in multiple contexts.

Conventions

This documentation uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Open-Source Software Included in Cisco ACE Application Control Engine

- Cisco ACE Application Control Engine includes the following open-source software, which is covered by the Apache 2.0 license (<http://www.apache.org/>): Ant, Apache Axis, Avalon Logkit, Commons, Ehcache, Globus Toolkit, Jetty, Log4J, Oro, Tomcat.
- Cisco ACE Application Control Engine includes the following open-source software, which is covered by The Legion of the Bouncy Castle (<http://www.bouncycastle.org/licence.html>) license: BouncyCastle.
- Cisco ACE Application Control Engine includes the following open-source software, which is covered by the GNU Lesser General Public License Version 2.1 (<http://www.gnu.org/licenses/lgpl.html>): c3p0-0.9.0.2.jar, Enterprise DT, Jasperreports 1.2, Jcommon 1.2, Jfreechart 1.0.1
- Cisco ACE Application Control Engine includes the following open-source software, which is covered by the Mozilla Public License Version 1.1 (<http://www.mozilla.org/MPL/MPL-1.1.html>): Itext 1.4.

Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

© 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
 “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



CHAPTER 1

Overview

This chapter contains the following sections:

- [ACE Appliance Device Manager Overview, page 1-1](#)
- [Information About the ACE No Payload Encryption Software Version, page 1-2](#)
- [Finding Information on CLI Tasks, page 1-3](#)
- [Logging into ACE Appliance Device Manager, page 1-4](#)
- [Changing Your Account Password, page 1-6](#)
- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Configuration Overview, page 1-18](#)
- [Understanding ACE Features, page 1-19](#)
- [IPv6 Considerations, page 1-20](#)
- [Understanding ACE Appliance Device Manager Terminology, page 1-22](#)

For more information on how to get started quickly, see the *Quick Start Guide, Cisco ACE 4700 Series Application Control Engine Appliance*.

ACE Appliance Device Manager Overview

The ACE Appliance Device Manager, which resides in flash memory on the ACE appliance, provides a browser-based interface for configuring and managing the ACE appliance. Its intuitive interface combines easy navigation with point-and-click provisioning of services, reducing the complexity of configuring virtual services and multiple feature sets.

ACE Appliance Device Manager menus and options:

- Supports end-to-end service provisioning of the ACE appliance and any associated virtual contexts, including network access, port management, application acceleration and optimization, load-balancing, SSL management, resource management, and fault tolerance.



Note

Device Manager uses SSH and XML over HTTPS to communicate with the ACE appliance and applying exec mode configuration changes (such as, checkpoint, SSL certificate, license, copy, and backup and restore configurations) to the appliance. By default, SSH is enabled on the appliance. However, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

- Helps you manage ACE appliance licenses and role-based access control (RBAC).
- Provides a monitoring interface with a flexible choice of statistics and graphs.
- Enables you report any problem with the ACE appliance using the Lifeline feature, which allows you to forward critical information about the problem to Cisco Technical Support.
- Offers task-based context-sensitive help from each screen, providing information about fields on the screen and related procedures.

For more information on how to get started quickly, see the *Getting Started Guide, Cisco ACE 4700 Series Application Control Engine Appliance*.

Information About the ACE No Payload Encryption Software Version

Beginning with ACE software Version A5(2.0), Cisco makes available the following two ACE software versions:

- **ACE Payload Encryption (PE)**—CLI commands related to payload encryption protocols are enabled. The ACE uses the payload encryption protocols to encrypt through-the-box traffic, such as IPsec, SSL VPN, and other secure voice protocols. The ACE PE software version contains the same payload encryption functionality found in previous ACE software versions.
- **ACE No Payload Encryption (NPE)**—CLI commands related to payload encryption protocols are either removed or do not function because the key encryption configuration commands have been removed. The new ACE NPE software version supports customers located in countries where the United States has imposed export restrictions on crypto functions. Without the use of payload encryption protocol commands, you cannot configure the ACE to perform data encryption tasks, such as configuring it as a virtual Secure Sockets Layer (SSL) server for SSL initiation or termination.

Modifications made to the ACE NPE software version do not affect management protocols, such as SSH, which is required to access the Device Manager GUI. For more information, see the “Using the Setup Script to Enable Connectivity to the Device Manager” section in the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

When using the ACE NPE software version, Device Manager includes the following modifications:

- The SSL configuration tab (Config > Virtual Contexts > SSL) is removed to prevent access to the main SSL configuration windows.
- In GUI sections that typically contain encryption-related configuration attributes, the attributes are either removed or you are not permitted to configure them. If you attempt to configure an encryption-related attribute, Device Manager does not allow you to deploy the configuration.
- In GUI sections that display monitored attributes that include encryption-related attributes (such as SSL connection rate), the encryption-related attributes may be listed but do not show any values associated with them.

This guide and the Device Manager online help contain notes where information about encryption-related attributes is affected when using the ACE NPE software version.

Finding Information on CLI Tasks

ACE Appliance Device Manager does not include a one-to-one mapping of all the possible command line interface (CLI) tasks for the ACE appliance. [Table 1-1](#) identifies some of the individual tasks to be performed from the CLI and provides a reference to the applicable configuration guide. For tasks not found in this table, see the *Getting Started Guide, Cisco ACE 4700 Series Application Control Engine Appliance*.

Table 1-1 *CLI Documentation References*

Task Topic	Related CLI Documentation
ARP, configuring	<i>Routing and Bridging Guide, Cisco ACE Application Control Engine</i> Chapter 5, Configuring ARP
Authentication and accounting (AAA) services	<i>Security Guide, Cisco ACE Application Control Engine</i> Chapter 2, Configuring Authentication and Accounting Services
Boot configuration (environment variable)	<i>Administration Guide, Cisco ACE Application Control Engine</i> Chapter 1, Setting Up the ACE
Date and time (time zone, daylight savings time, clock settings, and NTP)	<i>Administration Guide, Cisco ACE Application Control Engine</i> Chapter 1, Setting Up the ACE
LDAP directory server	<i>Security Guide, Cisco ACE Application Control Engine</i> Chapter 2, Configuring Authentication and Accounting Services
Message-of-the-day banner	<i>Administration Guide, Cisco ACE Application Control Engine</i> Chapter 1, Setting Up the ACE
Logging in to the ACE	<i>Administration Guide, Cisco ACE Application Control Engine</i> Chapter 1, Setting Up the ACE
RADIUS server	<i>Security Guide, Cisco ACE Application Control Engine</i> Chapter 2, Configuring Authentication and Accounting Services
script file ¹	<i>Command Reference, Cisco ACE Application Control Engine</i>
SSH management sessions	<i>Administration Guide, Cisco ACE Application Control Engine</i> Chapter 2, Enabling Remote Access to the ACE
TACACS+ server	<i>Security Guide, Cisco ACE Application Control Engine</i> Chapter 2, Configuring Authentication and Accounting Services
VLAN interfaces, configuring	<i>Routing and Bridging Guide, Cisco ACE Application Control Engine</i> Chapter 2, Configuring VLAN Interfaces

1. ACE Appliance Device Manager supports the domain object type Script for RBAC configuration. It does not configure the script CLI command. To use the script file command, use the ACE Appliance CLI to load a script into memory on the ACE and enable it for use.

**Note**

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

Logging into ACE Appliance Device Manager

You access ACE Appliance Device Manager features and functions through a Web-based interface. The following sections describe logging in, the interface, and terms used in ACE Appliance Device Manager.

By default, your ACE provides an Admin context and five user contexts, which allow you to use multiple contexts if you choose to configure them. ACE Appliance Device Manager uses Hypertext Transfer Protocol Secure (HTTPS) to securely encrypt HTTP requests and responses.

The ACE Appliance Device Manager login screen allows you to do the following:

- Log into the ACE Appliance Device Manager interface ([First Time Login, page 1-4](#) or [Logging In as a User, page 1-5](#))
- Change the password for your account (See [Changing Your Account Password, page 1-6](#).)
- Obtain online help by clicking **Help**

We recommend that before you log into the ACE Appliance Device Manager that you log in to the ACE appliance CLI and initially configure basic settings on the ACE. See the *Administration Guide, Cisco ACE Application Control Engine*, Chapter 1, Setting Up the ACE, for details.

**Note**

The DM does not support duplicate management IP addresses in different contexts.

First Time Login

After you perform the initial setup of the ACE appliance using the CLI, use the following procedure to log in the first time.

Procedure

- Step 1** Use a Web browser and navigate to the ACE Appliance Device Manager login screen by typing the IP address of the management interface configured during initial setup, such as `https://192.168.11.1`. A security alert screen appears.



Note The DM does not support duplicate management IP addresses in different contexts.

- Step 2** We recommend that you view the certificate to confirm it is from Cisco Systems, and then click **OK** or **Yes** to accept the certificate and proceed to the login screen. The keys you select may be different based on your browser.
- Step 3** In the User Name field, type **admin**.

The admin account was created when the system was installed. Once you are logged in using this account, you can create additional user accounts and manage virtual contexts, roles, and domains. For information on changing account passwords, see [Changing User Passwords, page 15-13](#).

- Step 4** In the Password field, type the password for the admin user account, **admin**. The password for the admin user account was configured when the system was installed. Change the default admin login password as outlined in [Changing Your Account Password, page 1-6](#).



Note All ACE appliances shipped from Cisco Systems are configured with the same administrative username and password. If you do not change the default Admin password, you will only be able to log in to the ACE through the console port.

- Step 5** Click **Login**.
When you log in, the default page that appears is the DM Homepage (see [Chapter 2, “Using Homepage”](#)).
- Step 6** We recommend you change your admin password. See [Changing Your Account Password, page 1-6](#).

Logging In as a User

Procedure

- Step 1** Use a web browser and navigate to the ACE Appliance Device Manager login screen by typing the IP address of the management interface of a virtual context you wish to login into, such as https://192.168.11.1. The login screen appears.



Note The DM does not support duplicate management IP addresses in different contexts.

- Step 2** To login as a user, enter **userid** in the User Name field (where *userid* is the login name provided by your admin).
- Step 3** Enter your password and click **Login**.

Related Topics

- [Changing Your Account Password, page 1-6](#)
- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Managing Users, page 15-7](#)
- [Managing User Roles, page 15-14](#)
- [Managing Domains, page 15-31](#)

Changing Your Account Password

All ACE appliances are shipped from Cisco Systems with the same administrative username and password. If you do not change the default Admin password, you will only be able to log in to the ACE through the console port.

Use this procedure to change your account password.

Procedure

- Step 1** Using a Web browser, navigate to the ACE Appliance Device Manager login screen by typing the IP address of the management interface configured during initial setup, such as `https://192.168.11.1`. The login screen appears.



Note The DM does not support duplicate management IP addresses in different contexts.

- Step 2** In the User Name field, enter your account user name.
- Step 3** Click **Change Password**. The Change Password configuration screen appears.
- Step 4** In the User Name field, enter the user name of the account you want to modify.
- For a user name in a context other than the Admin context, you must include the context name after the user name in the following format: `username@context_name`
- For example, for the test_1 user name in the C1 context, enter `test_1@C1`.
- Step 5** In the Old Password field, enter the current password for this account.
- Step 6** In the New Password field, enter the new password for this account.
- Password attributes such as minimum and maximum length or accepted characters are defined at the appliance level. Valid passwords are unquoted text strings with a maximum of 64 characters.
- Step 7** In the Confirm New Password field, reenter the new password for this account.
- Step 8** Do the following:
- Click **OK** to save your entries and to return to the login screen.
 - Click **Cancel** to exit this procedure without saving your entries and to return to the login screen.

Related Topics

- [Logging into ACE Appliance Device Manager, page 1-4](#)
- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Changing the Admin Password, page 15-13](#)

ACE Appliance Device Manager Interface Overview

When you log into the ACE Appliance Device Manager, the default window that appears is the Homepage from which you can access the operational and monitoring features of DM. For details about using Homepage, see [Chapter 2, “Using Homepage”](#).

Figure 1-1 is the All Virtual Contexts table (**Config > Virtual Contexts**) as an example of the DM interface components. Table 1-2 describes the numbered fields. A description of the buttons in the ACE Appliance Device Manager window are in Table 1-4 on page 1-9.

Features that are not accessible from your user login or context due to permission settings will not display or may display grayed out. For more details on roles and features, see [Managing User Roles](#), page 15-14.

Figure 1-1 ACE Appliance Device Manager Interface Components

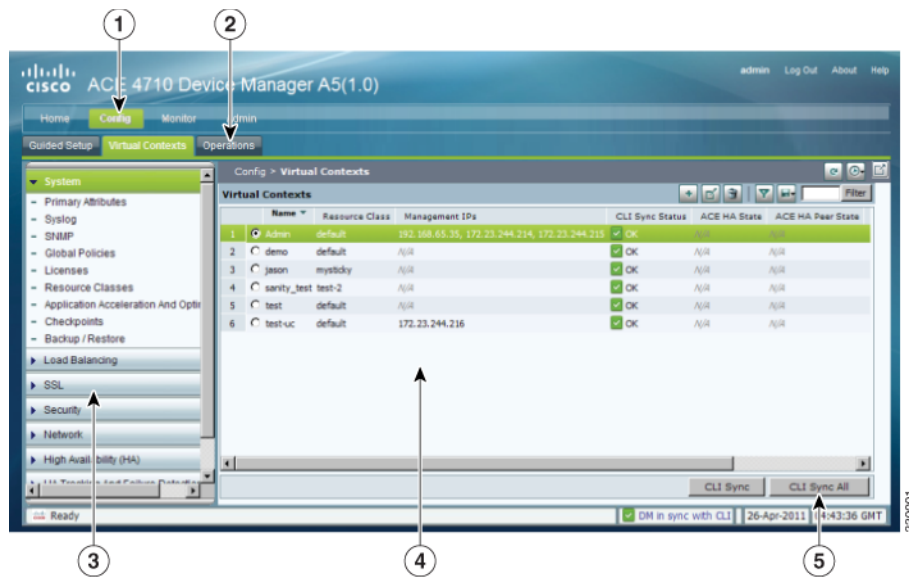


Table 1-2 ACE Appliance Device Manager Interface Components Descriptions

Field	Description
1	Navigation pane, which contains: <ul style="list-style-type: none"> The high-level navigation path within the ACE Appliance Device Manager interface, which includes Config, Monitor, and Admin functions. You can click a tab in the navigation path to view the next level of menus below the tabs. The Logout button. A Help menu that provides links to context-sensitive help and ACE Appliance Device Manager version information.
2	A second-level navigation path, which contains another level of navigation. Clicking an option in this submenu displays its associated menus in the navigation pane.
3	Third-level navigation pane, which contains additional levels of navigation. Clicking on the menu bar in this pane toggles the task menu display options.

Table 1-2 ACE Appliance Device Manager Interface Components Descriptions (continued)

Field	Description
4	Content area, which contains the display and input area of the window. It can include tables, graphical maps, configuration screens, graphs, buttons, or combinations of these items. For a description of buttons, see Table 1-4 on page 1-9 .
5	Status bar, which displays Device Manager and CLI synchronization information, polling status for a context, and the current date and time of the ACE appliance. Note Time values are displayed using a fixed time zone (GMT). The Device Manager automatically converts the timezone setting of the ACE appliance to GMT and displays the GMT string adjacent to the current time.

Related Topics

- [Understanding ACE Appliance Device Manager Screens and Menus, page 1-8](#)
- [Understanding Table Buttons, page 1-11](#)

Understanding ACE Appliance Device Manager Screens and Menus

Figure 1-2 contains many common screen elements as described in [Table 1-3](#).

Figure 1-2 Example ACE Appliance Device Manager Screen

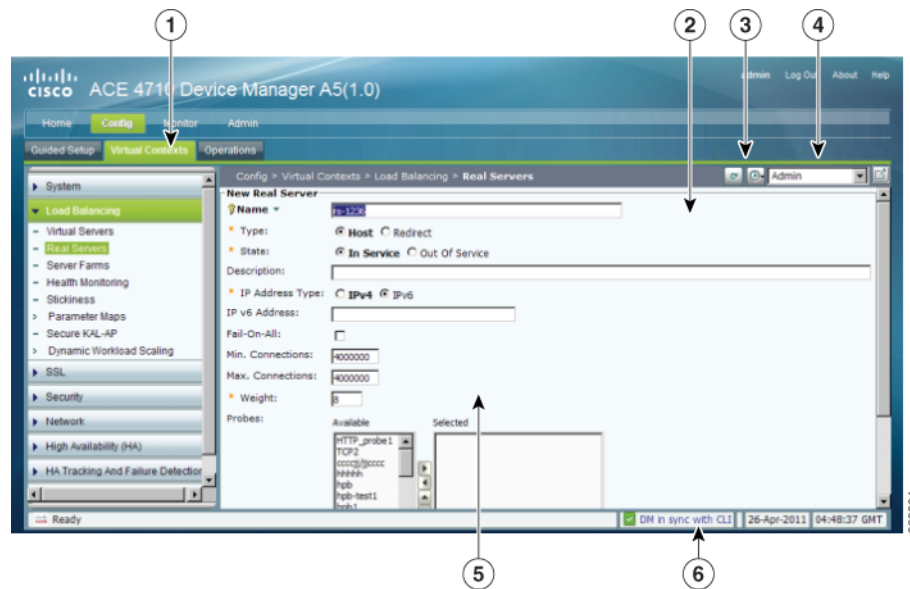


Table 1-3 Example ACE Appliance Device Manager Screen Descriptions

Number	Description
1	The high-level navigation path within the ACE Appliance Device Manager interface, which includes Config, Monitor, and Admin functions. You can click a tab in the navigation path to view the next level of menus below the tabs.
2	Content area. Contains the display and input area of the window. It can include tables, graphical maps, configuration screens, graphs, buttons, or combinations of these items.
3	Content buttons, which are described in Table 1-4 .
4	Object selector. Use this field to change virtual contexts.
5	Input fields. Use these fields to make selections and provide information. Fields with 2 or 3 options use radio buttons. Fields with more than 3 options use dropdown lists.
6	Synchronization and configuration section of the status bar. One indicator displays DM GUI and CLI synchronization and summary count information and the other indicator displays CLI synchronization information and polling status for a context. See Viewing Virtual Context Synchronization Status, page 4-80 for CLI Config Status message descriptions or Error Monitoring, page 14-15 for polling state message descriptions.

Related Topics

- [Understanding ACE Appliance Device Manager Buttons, page 1-9](#)
- [Understanding Table Buttons, page 1-11](#)
- [ACE Appliance Device Manager Screen Conventions, page 1-15](#)

Understanding ACE Appliance Device Manager Buttons

[Table 1-4](#) describes the buttons that appear in some of the Config, Monitor, and Admin screens.

**Note**

ACE Appliance Device Manager documentation, including online help, uses the names of buttons in all procedures. For example, “Click **Back** to return to the previous screen.”

Table 1-4 Button and Element Descriptions













Button	Name	Description
	Back	Returns you to the previous screen.
	Forward	Takes you to the screen previously visited from the current location.
	Refresh	Immediately refreshes the information in the content area with the current information.

Table 1-4 Button and Element Descriptions (continued)

Button	Name	Description
	Auto Refresh	Pauses the automatic refresh feature. You can pause the automatic refresh for 30, 60, 120, 300, 600, or 3600 seconds. If you disable the automatic refresh feature, ACE Appliance Device Manager times out after 30 minutes.
	Help	Launches context-sensitive help for the current screen.
	Add Another	Saves the current entries and refreshes the screen so you can add another entry.
	Advanced Editing Mode	Lets you view or enter advanced arguments for the selected display.
	Switch between Configure and Browse modes	Displays the subtables for those items that have additional sets of parameters that can be configured, such as Config > Virtual Contexts > context > Load Balancing > Server Farms . Note This button is not available on single-row tables such as Config > Virtual Contexts > System > SNMP . To switch between these modes, navigate to another screen where the button appears (for example, Config > Virtual Contexts > context > Load Balancing > Server Farms), click the button to enter the desired mode, and then return to the screen on which the button was missing. You will remain in the mode you selected.
	Key	Indicates that the associated field is a key field for this table. This field is mandatory and should be unique. If there are two fields with this key, then the combination must be unique.
	Plus	Displays a table with information related to the field where Plus appears. For example, when Plus appears next to the field label <i>Role</i> , clicking Plus displays a list of all Role Names in a separate window. Indicates that the associated field is a key field for this table. This field is mandatory and should be unique. If there are two fields with this key, then the combination must be unique. In File Browser only: expands or collapses the folder structure and reloads the specific directory.
	Screen Mode	Toggles from partial to full screen mode. Maximizes the content area and removes the navigation aids.
	Reorder List	Toggles list by alpha-order.







Related Topics

- [Understanding ACE Appliance Device Manager Screens and Menus, page 1-8](#)
- [Understanding Table Buttons, page 1-11](#)
- [ACE Appliance Device Manager Screen Conventions, page 1-15](#)

Understanding Table Buttons

When the content area of the ACE Appliance Device Manager screen contains a table, there are several buttons that appear as described in [Table 1-5](#).

Table 1-5 *ACE Appliance Device Manager Table Buttons*

Button	Name	Description
	Add	Lets you an entry to the displayed table.
	View/Edit	Opens the configuration screen of a selected entry in the table.
	Delete	Deletes the selected entry in the table.
	Filter	Filters the displayed list of items according to the criteria you specify. (See Filtering Entries, page 1-13 .)
	Go	Appears when filtering is enabled; updates the table with the filtering criteria.
	Save	Displays the current information in a new window in either raw data or Excel format so you can save it to a file or print it.

Related Topics

- [Understanding ACE Appliance Device Manager Buttons, page 1-9](#)
- [ACE Appliance Device Manager Screen Conventions, page 1-15](#)
- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Conventions in Tables, page 1-12](#)

Conventions in Tables

Selecting Table Entries

Double-clicking an entry in a table opens its corresponding configuration screen.

You can select multiple entries in a table in two ways:

- To select all table entries, check the check box at the top of the first column (where available).
- To select multiple entries individually, select the desired entries.

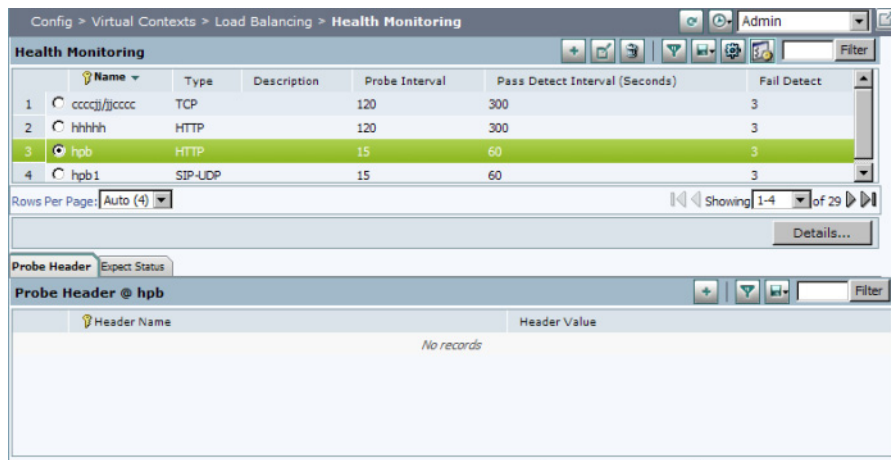
Parent Rows

If you select multiple entries in a table and then choose an option that can apply to only one entry at a time, the Parent Row field appears first in the configuration screen (see [Figure 1-3](#)).

The Parent Row field lists the selected entries and requires you to select one. Subsequent configuration choices in this screen are applied only to the entry identified in the Parent Row field.

Parent Row columns appear in subtables when multiple items are selected in the primary table.

Figure 1-3 Parent Rows in Configuration Screens

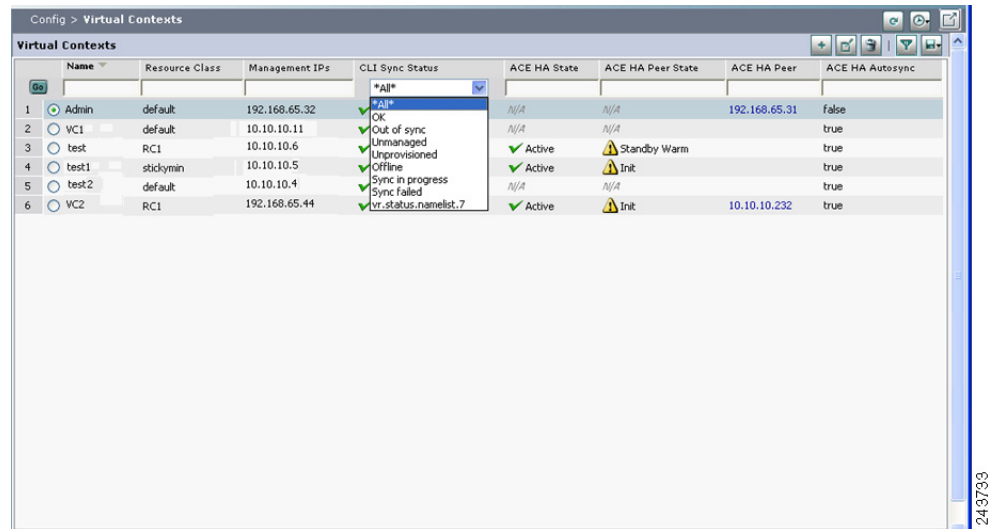


Filtering Entries

Click **Filter** to view table entries using criteria you select. When filtering is enabled, a filter row appears above the first table entry that allows you to filter entries in the following ways:

- In a drop-down list, select one of the ACE Appliance Device Manager-identified categories (see [Figure 1-4](#)). The table refreshes automatically with the entries that match the selected criterion.
- In fields without drop-down lists, enter the string you want to match, and then click **Go** above the first table entry. The table refreshes with the entries that match your input.

Figure 1-4 Example Table with Filtering Enabled



The screenshot shows the 'Config > Virtual Contexts' page. A table lists virtual contexts with columns: Name, Resource Class, Management IPs, CLI Sync Status, ACE HA State, ACE HA Peer State, ACE HA Peer, and ACE HA Autosync. A filter dropdown menu is open over the 'CLI Sync Status' column, showing options: 'All*', 'OK', 'Out of sync', 'Unmanaged', 'Unprovisioned', 'Offline', 'Sync in progress', 'Sync failed', and 'vr.status.name1st,7'. The table contains 6 entries.

	Name	Resource Class	Management IPs	CLI Sync Status	ACE HA State	ACE HA Peer State	ACE HA Peer	ACE HA Autosync
1	Admin	default	192.168.65.32	OK	N/A	N/A	192.168.65.31	false
2	VC1	default	10.10.10.11	Out of sync	N/A	N/A		true
3	test	RC1	10.10.10.6	Unmanaged	Active	Standby Warm		true
4	test1	stickymin	10.10.10.5	Offline	Active	Init		true
5	test2	default	10.10.10.4	Sync in progress	N/A	N/A		true
6	VC2	RC1	192.168.65.44	Sync failed	Active	Init	10.10.10.232	true

Related Topics

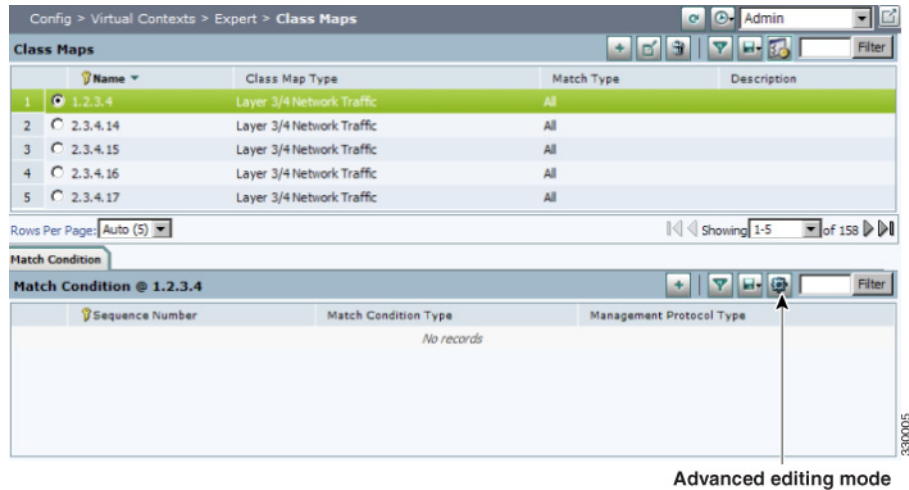
- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Using the Advanced Editing Option, page 1-14](#)

Using the Advanced Editing Option

By default, tables include columns that contain configured attributes, or a subset of columns related to a key field.

To view all configurable attributes in table format, click **Advanced Editing Mode** (the highlighted button in [Figure 1-5](#)). When advanced editing mode is enabled, all columns appear for your review (see [Figure 1-5](#)).

Figure 1-5 Advanced Editing Enabled Screen



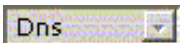
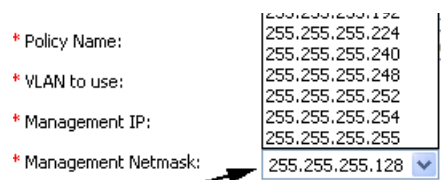
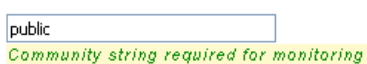


Related Topics

- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Conventions in Tables, page 1-12](#)

ACE Appliance Device Manager Screen Conventions

Table 1-6 describes other conventions used in ACE Appliance Device Manager screens.

Table 1-6 ACE Appliance Device Manager Screen Conventions

Convention	Example	Description
Dimmed field		Dimmed fields signify items that cannot be modified or that are not accessible from the current screen. Some buttons are dimmed if more than one item is selected in the list. For example, if multiple servers are selected in the Real Servers table, the View/Edit button is dimmed.
Dropdown lists		Fields with 2 or 3 options use radio buttons. Fields with more than 3 options use dropdown lists.
Light yellow field with green font		Warning text that appears below the affected field as green font against a light yellow background. In the example, a message stating that the community string must be entered if virtual context monitoring is used resulted in this display.
Red asterisk		A red asterisk indicates a required field.
Yellow field with red font		Incorrect, invalid, or incomplete entries appear as red font against a yellow background. In the example, an IP address cannot begin with four digits, resulting in this display. Warning text may also display below the affected field in green text on a yellow background.

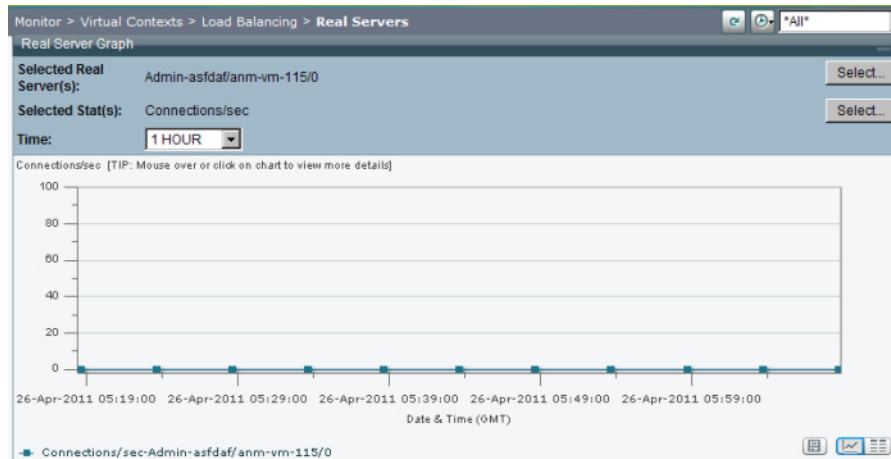
Related Topics

- [Conventions in Tables, page 1-12](#)
- [ACE Appliance Device Manager Interface Overview, page 1-6](#)

Viewing Monitoring Results

Figure 1-6 shows an example graph from the Monitor component.

Figure 1-6 Monitoring Results Screen



Monitor graphs offer many options including graph type, viewing raw data, graph layout, and values to be included. Table 1-7 identifies these options and their associated buttons. When viewing a graph, click the button to select the option. ACE Appliance Device Manager displays graph data in GMT.



Note

The maximum number of statistics that can be graphed is five.



Note

On the ACE, statistics are kept for 7 days or 20,000 hourly records, whichever comes first. The duration it takes to reach 20,000 hourly records is determined by the number of contexts, interfaces and real servers configured. The “All dates” graph provides all available data in the database, up to the above mentioned numbers. An ACE reboot will reset the statistics database.

Table 1-7 ACE Appliance Device Manager Monitor Buttons (unsure if all of these are still available)










Button	Name	Description
Graph Options		
	Line graph	Creates a line graph using the displayed information.
	Stacked bar graph	Creates a stacked bar chart using the displayed information.

Table 1-7 ACE Appliance Device Manager Monitor Buttons (unsure if all of these are still available)

Button	Name	Description
	Bar graph	Creates a bar graph using the displayed information.
Viewing Options		
	Show raw data	Displays the raw data in table format.
	Output to Excel	Displays the raw data in Excel format in a separate browser window.
Layout, Value, and Time Options		
	Change Legend Location	Displays the location of the legend.
	Multigraph Mode	Displays two line graphs next to each other.
	Value delta per time	Displays data points over time. See Monitoring Resource Usage, page 14-17 for a comparison of regular and value delta per time graphs. Time values are displayed using a fixed time zone (GMT).
	Time range	Displays the selected time range of the data to graph. Includes previous 1, 2, 8, or 24 hours or all dates.

Related Topics

- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Understanding ACE Appliance Device Manager Terminology, page 1-22](#)
- [Monitoring Resource Usage, page 14-17](#)

Configuration Overview

Use the flow chart in [Figure 1-7](#) to get started with the ACE Appliance Device Manager. [Table 1-8](#) describes these tasks in more detail.

Figure 1-7 *High-Level Configuration Process*

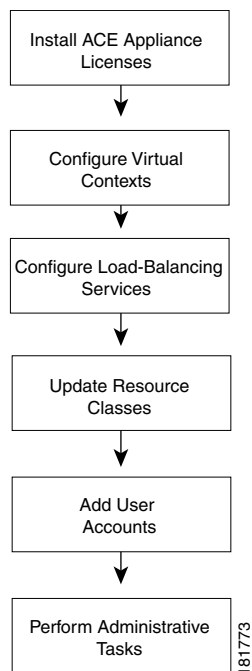


Table 1-8 *Configuration Task Overview*

	Task	Description
Step 1	Install ACE appliance licenses.	In this step you install licenses for ACE appliances that let you increase the number of virtual contexts, appliance bandwidth, and SSL TPS (transactions per second). See Managing ACE Appliance Licenses, page 4-29 for details.
Step 2	Configure virtual contexts.	In this step you partition the ACE appliance into multiple virtual devices or <i>contexts</i> . Each context contains its own set of policies, interfaces, resources, and administrators, allowing you to efficiently manage resources, users, and the services you provide to your customers. See Using Virtual Contexts, page 4-2 for details.
Step 3	Configure load-balancing services.	In this step you configure load balancing to manage client requests for service. See Load Balancing Overview, page 5-1 for details.
Step 4	Update resource classes.	In this step you configure resource usage models that you can apply across your network. See Managing Resource Classes, page 4-35 for details.

Table 1-8 Configuration Task Overview (continued)

	Task	Description
Step 5	Add user accounts.	In this step you set up tiered access for users. See Managing the ACE Appliance, page 15-1 for details.
Step 6	Perform administrative tasks.	This step includes ongoing maintenance and administrative tasks, such as follows: <ul style="list-style-type: none"> Updating ACE appliance software (see Managing ACE Appliance Licenses, page 4-29). Monitoring virtual context or ACE Appliance Device Manager statistics (see “Monitoring Your Network” section on page 14-1).

Understanding ACE Features

The ACE performs high-performance server load balancing (SLB) among groups of servers, server farms, firewalls, and other network devices, based on Layer 3 as well as Layer 4 through Layer 7 packet information. The ACE provides the following major features and functionality.

- **Ethernet Interfaces**—The ACE provides four physical Ethernet ports that provide an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks. Each Layer 2 Ethernet port supports autonegotiate, full-duplex, or half-duplex operation on an Ethernet LAN, and can carry traffic within a designated VLAN interface.
- **Routing and Bridging**—You configure the corresponding VLAN interfaces on the ACE as either routed or bridged. When you configure an IP address on an interface, the ACE automatically configures it as a routed mode interface. When you configure a bridge group on an interface VLAN, the ACE automatically configures it as a bridged interface.
- **Traffic Policies**—The ACE allows you to perform advanced administration tasks such as using traffic policies to classify traffic flow and the action to take for the type of traffic. Traffic policies consist of class maps, policy maps, and service policies.
- **Redundancy**—Redundancy provides fault tolerance for the stateful switchover of flow, and offers increased uptime for a more robust network.
- **Virtualization**—Virtualization allow you to manage ACE system resources and users, as well as the services provided to your customers. Multiple contexts use the concept of virtualization to partition your ACE into multiple virtual devices or contexts. Each context contains its own set of policies, interfaces, resources, and administrators.
- **Server Load Balancing**—Server load balancing (SLB) on the ACE provides network traffic policies for SLB, real servers and server farms, health monitoring through probes, and firewall load balancing.
- **ACE Security Features**—The ACE contains several security features including ACLs, NAT, user authentication and accounting, HTTP deep packet inspection, FTP command request inspection, and application protocol inspection of DNS, HTTP, ICMP, or RTSP.
- **Secure Sockets Layer**—The SSL protocol on the ACE provides encryption technology for the Internet, ensuring secure transactions.

- **Application Acceleration and Optimization**—The ACE includes several optimization technologies to accelerate Web application performance, optimize network performance, and improve access to critical business information.
- **Command-Line Interface**—The command-line interface (CLI) is a line-oriented user interface that provides commands for configuring, managing, and monitoring the ACE. For more information, see the *Command Reference, Cisco ACE Application Control Engine*.

Related Topics

- [ACE Appliance Device Manager Overview, page 1-1](#)
- *Command Reference, Cisco ACE Application Control Engine*

IPv6 Considerations

The DM supports IPv6 configurations with the following considerations:

- By default, IPv6 is disabled on an interface. You must enable IPv6 on the interface to enable its configured IPv6 addresses. The interface cannot be in bridged mode. The interface may or may not have IPv4 addresses configured on it.
- When you enable IPv6 or configure a global IPv6 address on an interface, the ACE automatically does the following:

- Configures a link-local address (if it is not already configured)
- Performs duplicate address detection (DAD) on both addresses

You must enable IPv6 on the interface to enable global IPv6 address.

- IPv6 on interface can be individually enabled or disabled. IPv6 cannot be enable or disable globally.
- A link-local address is an IPv6 unicast address that has a scope of the local link only and is required on every interface. Every link-local address has a predefined prefix of FE80::/10. You can configure a link-local address manually. If you do not configure a link-local address before enabling an IPv6 address on the interface, the ACE automatically generates a link-local address with a prefix of FE80::/64. Only one IPv6 link-local address can be configured on an interface.

In a redundant configuration, you can configure an IPv6 peer link-local address for the standby ACE. You can configure only one peer link-local address on an interface.

- A unique-local address is an optional IPv6 unicast address that is used for local communication within an organization and it is similar to a private IPv4 address (for example, 10.10.2.1). unique-local addresses have a global scope, but they are not routable on the internet, and they are assigned by a central authority. All unique-local addresses have a predefined prefix of FC00::/7. You can configure only one IPv6 unique-local address on an interface.

In a redundant configuration, you can configure an IPv6 peer unique-local address on the active that is synchronized to the standby ACE. You can configure only one peer unique-local IPv6 address on an interface.

- A global address is an IPv6 unicast address that is used for general IPv6 communication. Each global address is unique across the entire Internet. Therefore, its scope is global. The low order 64 bits can be assigned in several ways, including autoconfiguration using the EUI-64 format. You can configure only one globally unique IPv6 address on an interface.

In a redundant configuration, you can configure an IPv6 peer global address that is synchronized to the standby ACE.

When you configure redundancy with active and standby ACEs, you can configure a VLAN interface that has an alias global IPv6 address that is shared between the active and standby ACEs. The alias IPv6 address serves as a shared gateway for the two ACEs in a redundant configuration. You can configure only one alias global IPv6 address on an interface.

- A multicast address is used for communications from one source to many destinations. IPv6 multicast addresses function in a manner that is similar to IPv4 multicast addresses. All multicast addresses have a predefined prefix of FF00::/8.
- The ACE supports abbreviated IPv6 addresses. When using double colons (::) for leading zeros in a contiguous block, they can only be used once in an address. Leading zeros can be omitted. Trailing zeros cannot be omitted. The DM will abbreviate an IPv6 address after you finish typing it. If you enter the entire address with a block of contiguous zeros, the DM collapses it into the double colons. For example: FF01:0000:0000:0000:0000:0000:101 becomes FF01::101.
- The ACE uses the Neighbor Discovery (ND) protocol to manage and learn the mapping of IPv6 to Media Access Control (MAC) addresses of nodes attached to the local link. The ACE uses this information to forward and transmit IPv6 packets. The neighbor discovery protocol enables IPv6 nodes and routers to:
 - Determine the link-layer address of a neighbor on the same link
 - Find neighboring routers
 - Keep track of neighbors

The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and keep track of neighbor routers. The IPv6 neighbor discovery process uses the following mechanisms for its operation:

- Neighbor Solicitation
- Neighbor Advertisement
- Router Solicitation
- Router Advertisement
- Duplicate Address Detection
- The ACE supports IPv6-to-IPv6 L4/L7 SLB, including support for IPv6 VIP, predictor, probe, server farm, sticky, access-list, object-group, interface, source NAT, OCSP, and CRL.
- The probe must have the same IP address type (IPv6 or IPv4) as the real server. For example, you cannot configure an IPv6 probe to an IPv4 real server.
- You can associate both IPv6 and IPv4 probes to a server farm.
- Only the following Layer 7 protocol will support IPv6:
 - Layer 7 HTTP/HTTPS/DNS
 - Layer 4 TCP/UDP
- The ACE supports the following:
 - IPv6-to-IPv4 SLB and IPv4-to-IPv6 SLB for L7 HTTP/HTTP/TCP/UDP
 - Source NAT support of IPv6
 - IPv6 access-list and object group
 - DHCPv6 relay

- ICMPv6 traffic is not automatically allowed. You must configure the corresponding management traffic policy to allow the ping request to ACE. However, the necessary ND (neighbor Discovery) messages for ARP, duplication address detection are automatically permitted.
- All the management traffic used by the network management server or DM is required to send over IPv4 protocol. IPv6 is not supported.
- Copying files over IPv6 to or from devices are not supported.
- The ACE supports IPv6 HA:
 - All the FT transport (ft vlan) is still on IPv4.
 - Track IPv6 host /peer will be supported

Understanding ACE Appliance Device Manager Terminology

It is useful to understand the following terms when using the ACE Appliance Device Manager:

- Virtual context

A virtual context is a concept that allows users to partition an ACE appliance into multiple virtual devices. Each virtual context contains its own set of policies, interfaces, and resources, allowing administrators to more efficiently manage system resources and services.

- Virtual server

In a load-balancing environment, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. A virtual server is bound to physical services running on real servers in a server farm and uses IP address and port information to distribute incoming client requests to the servers in the server farm according to a specified load-balancing algorithm.

- Role-Based Access Control

Managing users using role-based access allows administrators to set up users, roles, and domain access to your virtual contexts. Each user is assigned a role and a domain which defines what virtual contexts they can view and configure. Roles determine which commands and resources are available to a user. Domains determine which objects they can use. Only users associated with an admin virtual context are allowed to see other virtual contexts.

There are two types of virtual contexts:

- Admin context

The Admin context, which contains the basic settings for each virtual device or context, allows a user to configure and manage all contexts. When a user logs into the Admin context, he or she has full system administrator access to the entire ACE appliance and all contexts and objects within it. The Admin context provides access to network-wide resources, for example, a syslog server or context configuration server. All global commands for ACE appliance settings, contexts, resource classes, and so on, are available only in the Admin context.

- User context

A user context has access to the resources in which the context was created. For example, a user context that was created by an administrator while in the Admin context, by default, has access to all resources in an ACE appliance. Any user created by someone in a user-defined context only has access to the resources within that context. In addition, roles and domains create access parameters for each user. For a description of the predefined user roles, see [Managing User Roles, page 15-14](#).

For more information on RBAC, see [Controlling Access to the Cisco ACE Appliance, page 15-3](#).

- Resource class

A resource class is a defined set of resources and allocations available for use by a virtual context. Using resource classes prevents a single context from using all available resources and can be used to ensure that every context is guaranteed the minimum set of resources necessary.

Related Topics

- [Controlling Access to the Cisco ACE Appliance, page 15-3](#)
- [ACE Appliance Device Manager Interface Overview, page 1-6](#)
- [Conventions in Tables, page 1-12](#)
- [Glossary](#)

Supported Browsers for ACE Appliance Device Manager

The ACE appliance Device Manager is supported on the following browsers listed in [Table 9](#). All browsers require cookies and DHTML (JavaScript) to be enabled.

Table 9 *Supported Browsers*

Browser	Version	Client Platform
Microsoft Internet Explorer	IE 7.0	Windows XP Professional with Service Pack 2 or Windows Vista with Service Pack 1
	IE 8.0	Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, or Windows 7
Firefox	20	<ul style="list-style-type: none">• Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, or Windows 7• Red Hat Enterprise Linux 5



CHAPTER 2

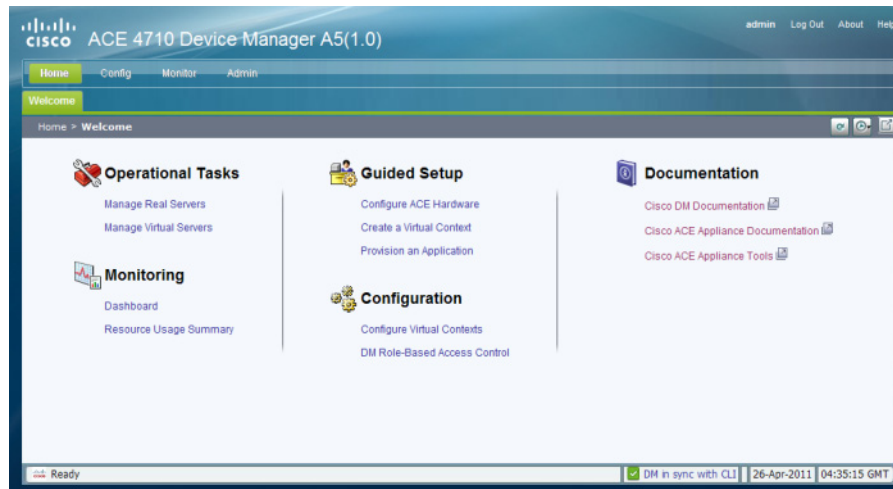
Using Homepage

Homepage is a launching point for quick access to selected areas within Cisco Device Manager (DM). It allows you to have quick access to the following operations and guided setup tasks in DM:

- Operational tasks that you can access:
 - The Real Servers table to view information for each configured real server, activate or suspend real servers listed in the table, or modify the server weight.
 - The Virtual Servers table to view information for each configured virtual server and to activate or suspend virtual servers listed in the table.
- Monitoring—View the system dashboard for health, usage, and performance information related to the ACE appliance, and system traffic resource usage.
- Guided setup tasks that you can launch:
 - The Cisco Application Control Engine (ACE) Hardware Setup task to configure ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability (HA) deployments.
 - The Virtual Context Setup task to create and connect an ACE virtual context.
 - The Application Setup task to configure end-to-end load-balancing for your application.
- Configuration—Tasks that allow you to configure system attributes for a virtual context, and control a user's access to the ACE.
- Documentation—Quick links to DM and ACE appliance user documentation on www.cisco.com, and the local ACE appliance toolpage.

The DM Homepage (see [Figure 2-1](#)) is the first page that appears in DM after you log in.

Figure 2-1 *Homepage Window*



[Table 2-1](#) identifies the Homepage links, associated pages in DM, and related topics that can be found in this document.

Table 2-1 *Homepage Links*

Homepage Link	DM Page	Related Topics
Operational Tasks		
Manage Real Servers	Config > Operations > Real Servers	Managing Real Servers, page 6-9
Manage Virtual Servers	Config > Operations > Virtual Servers	Managing Virtual Servers, page 5-63
Monitoring		
Dashboard	Monitor > Virtual Contexts > Dashboard > System Dashboard	ACE System Dashboard, page 14-3
Resource Usage Summary	Monitor > Virtual Contexts > Resource Usage > Connections	Monitoring System Traffic Resource Usage, page 14-19
Guided Setup		
Configure ACE Hardware	Config > Guided Setup > ACE Hardware Setup	Using ACE Hardware Setup, page 3-3
Create a Virtual Context	Config > Guided Setup > Virtual Context Setup	Using Virtual Context Setup, page 3-7
Provision an Application	Config > Guided Setup > Application Setup	Using Application Setup, page 3-9
Configuration		
Configure Virtual Contexts	Config > Virtual Contexts	Configuring Virtual Context Primary Attributes, page 4-11
DM Role-Based Access Control	Adman > Role-Based Access Control > Users	Managing Users, page 15-7

Table 2-1 Homepage Links (continued)

Homepage Link	DM Page	Related Topics
Documentation		
Cisco DM Documentation (link to documentation set on www.cisco.com)	N/A	N/A
Cisco ACE Appliance Documentation (link to documentation set on www.cisco.com)	N/A	N/A
Cisco ACE Appliance Tools (link to the local ACE appliance toolpage)	N/A	N/A



CHAPTER 3

Using DM Guided Setup

This chapter describes how to use Cisco Device Manager (DM) Guided Setup.



Note

When naming ACE objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), enter an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you are using DM with an ACE appliance and you configure a named object at the ACE CLI, keep in mind that DM does not support all of the special characters that the ACE CLI allows you to use when configuring a named object. If you use special characters that DM does not support, you may not be able to import or manage the ACE using DM.

This chapter contains the following sections:

- [Information About Guided Setup, page 3-1](#)
- [Guidelines and Limitations, page 3-3](#)
- [Using ACE Hardware Setup, page 3-3](#)
- [Using Virtual Context Setup, page 3-7](#)
- [Using Application Setup, page 3-9](#)

Information About Guided Setup

DM Guided Setup provides a series of setup sequences that offer GUI window guidance and networking diagrams to simplify the configuration of DM and the network devices that it manages.

Guided Setup allows you to quickly perform the following tasks:

- Configure ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability (HA) deployments.
- Create and connect to an ACE virtual context.
- Set up load balancing application from an ACE to a group of back-end servers.

To access Guided Setup, click the Config tab located at the top of the window, and then click Guided Setup.

**Note**

The available menu and button options on the Guided Setup tasks are under Role-Based Access Control (RBAC). Menu and button options will be grayed if proper permission has not been granted to the logged in user by the administrator. See the [“Controlling Access to the Cisco ACE Appliance”](#) section on [page 15-3](#) for more information about RBAC in DM.

[Table 3-1](#) identifies the individual guided setup tasks and related topics.

Table 3-1 *Guided Setup Tasks and Related Topics*

Guided Setup Tasks	Purpose	Related Topics
ACE hardware setup	Launch the ACE Hardware Setup task to help you configure ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability (HA) deployments.	<ul style="list-style-type: none"> • Using ACE Hardware Setup, page 3-3 • Managing ACE Appliance Licenses, page 4-29 • Configuring SNMP for Virtual Contexts, page 4-19 • Configuring Port Channel Interfaces, page 10-2 • Configuring Gigabit Ethernet Interfaces, page 10-5 • Configuring Virtual Context VLAN Interfaces, page 10-10 • Configuring High Availability Peers, page 11-8
Virtual context setup	Launch the Virtual Context Setup task to create and connect an ACE virtual context.	<ul style="list-style-type: none"> • Using Virtual Context Setup, page 3-7 • Managing Resource Classes, page 4-35 • Creating Virtual Contexts, page 4-2 • Configuring Virtual Contexts, page 4-7
Application setup	Launch the Application Setup task to configure load balancing for your application. This task guides you through a complete end-to-end configuration of the ACE for many common server load-balancing situations.	<ul style="list-style-type: none"> • Using Application Setup, page 3-9 • Configuring Virtual Context VLAN Interfaces, page 10-10 • Configuring Virtual Context BVI Interfaces, page 10-23 • Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32 • Configuring Security with ACLs, page 4-58 • SSL Setup Sequence, page 9-5 • Configuring Virtual Servers, page 5-2

Guidelines and Limitations

As you perform a Guided Setup task, use the following operating conventions:

- To move between steps, click the name of the step in the menu to the left.
- The steps for each task are listed in an order that is designed to prevent problems during later steps; however, you can skip steps if you know they are not applicable to your application.
- Depending on your user privileges, DM may prevent you from making changes on certain steps.
- You must save and deploy any changes you want to keep before leaving each page.
- Each task can be run as many times as you like.

Using ACE Hardware Setup

You can use the ACE Hardware Setup task to configure ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability (HA) deployments.

Assumptions

- You can extend the functionality of the ACE by installing licenses. If you plan to extend the ACE functionality, ensure that you have received the proper software license key for the ACE, that ACE licenses are available on a remote server for importing to the ACE, or you have received the software license key and have copied the license file to the disk0: file system on the ACE using the **copy path/filename1 disk0:** CLI command.



Note See the *Administration Guide, Cisco ACE Application Control Engine* for details on the **copy path/filename1 disk0:** CLI command.

- You must be in the Admin virtual context on an ACE appliance to configure ACE devices that are new to the network.
- When importing an ACE HA pair into DM, you should follow one of the following configuration requirements so that DM can uniquely identify the ACE HA pair:
 - Use a unique combination of FT interface VLAN and FT IP address/peer IP address for every ACE HA pair imported into DM. For HA, it is critical that the combination of FT interface VLAN and IP address/peer IP address is always unique across every pair of ACE peer devices.
 - Define a peer IP address in the management interface using the management IP address of the peer ACE (module or appliance). The management IP address and management peer IP address used for this definition should be the management IP address used to import both ACE devices into DM.



Note For more information about the use of HA pairs imported into DM, see the [“Understanding ACE Redundancy” section on page 11-2](#).

- When you are configuring the ACE, changes to the physical interfaces (including Gigabit Ethernet ports or port channels) can result in a loss of connectivity between DM and the ACE. Use caution when following the ACE Hardware Setup task if you are modifying the interface that management traffic is traversing.

Procedure

Step 1 Choose **Config > Guided Setup > ACE Hardware Setup**.

The ACE Hardware Setup window appears with the Configuration Type drop-down list.

Step 2 From the Configuration Type drop-down list, choose whether to set up the ACE as a standalone device or as a member of a high-availability (HA) ACE pair:

- Standalone—The ACE is not to be used in an HA configuration.
- HA Secondary—The ACE is to be the secondary peer in an HA configuration.
- HA Primary—The ACE is to be the primary peer in an HA configuration.



Note Ensure that you complete the ACE hardware setup task for the secondary device *before* you set up the primary device.

Step 3 Click **Start Setup**.

The License window appears (Config > Guided Setup > ACE Hardware Setup > Licenses). Cisco offers licenses for ACE appliances that allows you to increase the number of default contexts, bandwidth, and SSL TPS (transactions per second). For more information, see the *Administration Guide, Cisco ACE Application Control Engine* on cisco.com.

If you need to install licenses at this point, go to Step 4.

If you do not need to install licenses at this point, go to Step 5.

Step 4 Install one or more ACE licenses (see the “[Managing ACE Appliance Licenses](#)” section on page 4-29).



Note For an ACE primary and secondary HA pair, because each ACE license is only valid on a single hardware device, licenses are not synchronized between HA peer devices. You must install an appropriate version of each license independently on both the primary and secondary ACE devices.

Step 5 Click **SNMP v2c Read-Only Community String** under ACE Hardware Setup (Config > Guided Setup > ACE Hardware Setup > SNMP v2c Read-Only Community String).

The SNMP v2c Read-Only Community String window appears.

Perform the following actions to configure an SNMP community string (a requirement for an ACE to be monitored by DM):

- a. Click **Add (+)** at the top of the SNMP v2c Read-Only Community String table to create an SNMP community string. The New SNMP v2c Community window appears.



Note For DM to monitor an ACE, you must configure an SNMPv2c community string in the Admin virtual context.

- b. In the Read-Only Community field, enter the SNMP read-only community string name. Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.

Additional SNMP configuration selections are available under Config > Virtual Contexts > *context* > System > SNMP. See the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19.

- Step 6** If you are configuring an ACE appliance, to group physical ports together on the ACE appliance to form a logical Layer 2 interface called the port-channel (sometimes known as EtherChannels), click **Port Channel Interfaces** under ACE Hardware Setup.

The Port Channel Interfaces window appears (Config > Guided Setup > ACE Hardware Setup > Port Channel Interfaces).



Note You must configure port channels on both the ACE appliance and the switch that the ACE is connected to.

Perform the following actions to configure a port channel interface:

- a. At the top of the Port Channel Interfaces table, click **Add (+)** to add a port channel interface, or choose an existing port channel interface and click **Edit** to modify it. The New Port Channel Interface window appears.



Note If you click Edit, not all of the fields can be modified.

- b. Enter the port channel interface attributes as described in the [“Configuring Port Channel Interfaces” section on page 10-2](#).
- c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- d. To display statistics and status information for a port-channel interface, choose the interface from the Port Channel Interfaces table and click **Details**. The **show interface port-channel** CLI command output appears. See the [“Displaying Port Channel Interface Statistics and Status Information” section on page 10-5](#) for details.

- Step 7** If you are configuring an ACE appliance, to configure one or more of the Gigabit Ethernet ports on the appliance, click **GigabitEthernet Interfaces** under ACE Hardware Setup. The GigabitEthernet Interfaces window appears (Config > Guided Setup > ACE Hardware Setup > GigabitEthernet Interfaces).

- a. Choose an existing Gigabit Ethernet interface and click **Edit** to modify it.
- b. Enter the Gigabit Ethernet physical interface attributes as described in the [“Configuring Gigabit Ethernet Interfaces” section on page 10-5](#).
- c. Click **Deploy Now** when completed to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- d. Repeat Steps a through c for each Gigabit Ethernet interface that you want to configure.
- e. To display statistics and status information for a particular Gigabit Ethernet interface, choose the interface from the GigabitEthernet Interfaces table, and then click **Details**. The **show interface gigabitEthernet** CLI command output appears. See the [“Displaying Gigabit Ethernet Interface Statistics and Status Information” section on page 10-9](#) for details.

- Step 8** If the ACE is a member of an HA ACE pair, click **VLAN Interfaces** under ACE Hardware Setup.

The VLAN Interfaces window appears (Config > Guided Setup > ACE Hardware Setup > VLAN Interfaces).

**Note**

To prevent loss of management connectivity during an HA configuration, you must configure the IP addresses of the management VLAN interface correctly for your HA setup. During this procedure, choose the management VLAN interface (and click the **Edit** button) and make sure its IP address, alias IP address, and peer IP address are all set correctly. You can repeat this process for any VLAN interfaces that you want. If the management VLAN is properly configured before establishing HA, you will be able to return later to reconfigure other VLANs.

- a. Click **Add** to add a new VLAN interface, or choose an existing VLAN interface and click **Edit** to modify it.

**Note**

If you click Edit, not all of the fields can be modified.

- b. Enter the VLAN interface attributes as described in the [“Configuring Virtual Context VLAN Interfaces” section on page 10-10](#). Click **More Settings** to access the additional VLAN interface attributes. By default, DM hides the default VLAN interface attributes and the VLAN interface attributes which are not commonly used.
- c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- d. To display statistics and status information for a VLAN interface, choose the VLAN interface from the VLAN Interface table, and then click **Details**. The **show interface vlan**, **show ipv6 interface vlan**, and **show ipv6 neighbors** CLI commands appear. Click on the command to display its output. See the [“Displaying VLAN Interface Statistics and Status Information” section on page 10-23](#) for details.

Step 9 If the ACE is the primary peer in a high availability (HA) configuration, click **HA Peering** under ACE Hardware Setup (Config > Guided Setup > ACE Hardware Setup > HA Peering).

- a. Click **Edit** below the HA Management section to configure the primary ACE and the secondary ACE as described in the [“Configuring High Availability Peers” section on page 11-8](#). There are two columns, one for the selected ACE and another for a peer ACE.

You can specify the following information:

- Identify the two members of a HA pair.
- Assign IP addresses to the peer ACEs.
- Assign an HA VLAN to HA peers and bind a physical Gigabit Ethernet interface to the FT VLAN.
- Configure the heartbeat frequency and count on the peer ACEs in a fault-tolerant VLAN.

When completed, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

- b. Click **Add** below the ACE HA group table to add a new high availability group. Enter the information in the configurable fields as described in the [“Configuring High Availability Peers” section on page 11-8](#). When completed, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

The HA State field displays FT VLAN Compatible once HA setup has been successfully completed.

**Note**

To display statistics and status information for a particular HA group, choose the group from the ACE HA Groups table and click **Details**. The **show ft group group_id detail** CLI command output appears. See the [“Displaying High Availability Group Statistics and Status Information” section on page 11-16](#) for details.

- Step 10** Once the HA State field in the ACE HA Groups table shows a successful state, the ACE is ready for further configuration as follows:
- To set up additional virtual contexts, continue to the Virtual Context Setup task to create and connect an ACE virtual context. See the [“Using Virtual Context Setup” section on page 3-7](#).
 - To set up an application in an existing virtual context, continue to the Application Setup task to set up load-balancing for an application from an ACE to a group of back-end servers. See the [“Using Application Setup” section on page 3-9](#).

Related Topics

- [Managing ACE Appliance Licenses, page 4-29](#)
- [Configuring SNMP for Virtual Contexts, page 4-19](#)
- [Configuring Port Channel Interfaces, page 10-2](#)
- [Configuring Gigabit Ethernet Interfaces, page 10-5](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring High Availability Peers, page 11-8](#)

Using Virtual Context Setup

You can use the Virtual Context Setup task to create and connect an ACE virtual context. Virtual contexts use virtualization to partition your ACE appliance into multiple virtual devices, or contexts. Each context contains its own set of policies, interfaces, resources, and administrators.

Before You Begin

You must be in the Admin context on the ACE to create a new user context.

Procedure

- Step 1** Choose **Config > Guided Setup > Virtual Context Setup**.
The Virtual Context Setup window appears.
- Step 2** From the ACE Device drop-down list, choose an ACE.
- Step 3** Click **Start Setup**.
The Resource Classes window appears (Config > Guided Setup > Virtual Context Setup > Resource Classes).

Perform the following tasks to create or modify a resource class:

- a. If you want to create a resource class, click **Add (+)**. The New Resource Class configuration window appears. Enter the resource information as described in the [“Managing Resource Classes” section on page 4-35](#).
- b. If you want to modify an existing resource, choose the resource class that you want to modify, and then click **Edit**. The Edit Resource Class configuration window appears. Enter the resource information as described in the [“Managing Resource Classes” section on page 4-35](#).
- c. Click **OK** to save your entries and to return to the Resource Classes table.

Make note of the resource class that you want to use because you will need it in Step 5.

Step 4 Click **Virtual Context Management** under Virtual Context Setup.

The Virtual Context window appears (Config > Guided Setup > Virtual Context Setup > Virtual Context Management).

Perform the following actions to create or modify a virtual context:

- a. If you want to create a virtual context, click **Add (+)**. The New Virtual Context window appears. Configure the virtual context as described in the [“Configuring Virtual Contexts” section on page 4-7](#).
- b. If you want to modify an existing virtual context, choose the virtual context that you want to modify and click **Edit**. The Primary Attributes configuration screen appears. Enter the primary attributes for this virtual context as described in the [“Configuring Virtual Context Primary Attributes” section on page 4-11](#).

Step 5 When completed, click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files. Follow these guidelines when creating or modifying the virtual context:

- To connect the virtual context to the available VLANs, specify one or more VLANs in the Allocated VLANs field. You can specify multiple VLAN values and ranges (for example, “10, 14, 70-79”).
- For virtual contexts configured for an ACE, you must set up all VLANs used in this step as trunk or access VLANs on the port channel or Gigabit Ethernet interfaces. If you did not set up these VLANs during the ACE Hardware Setup task, you can return to the ACE Hardware Setup window to configure the required VLANs. See the [“Using ACE Hardware Setup” section on page 3-3](#).
- When specifying the resource class for the virtual context, choose the resource class that you created or specified in Step 3.



Note If you are unsure of the resource class to use for this virtual context, choose **default**. You can change the resource class setting at a later time.

- If HA has been correctly configured for this ACE device, the High Availability check box will be checked. If the check box is unchecked, check it to instruct DM to automatically configure synchronization for this virtual context.



Note The High Availability check box is available only if HA Peering has previously been completed for the ACE hardware.

- If you want to set up a separate management VLAN interface for the virtual context, under Management Settings, configure the management interface for this virtual context and create an admin user. Each context also has its own management VLAN that you can access using the DM GUI. In this case, you would assign an independent VLAN and IP address for management traffic to access the virtual context.

Step 6 To edit the load-balancing configuration for a virtual context, continue to the Application Setup task. See the [“Using Application Setup” section on page 3-9](#).

Related Topics

- [Using ACE Hardware Setup, page 3-3](#)
- [Using Virtual Contexts, page 4-2](#)
- [Managing Resource Classes, page 4-35](#)
- [Creating Virtual Contexts, page 4-2](#)
- [Configuring Virtual Contexts, page 4-7](#)
- [Using Application Setup, page 3-9](#)

Using Application Setup

This section contains the following topics:

- [ACE Network Topology Overview, page 3-9](#)
- [Using Application Setup, page 3-10](#)

ACE Network Topology Overview

With respect to ACE configuration, the network topology describes where—which VLAN or subnet—client traffic comes into the ACE and where this traffic is sent to real servers. Network configuration for ACE load balancing depends on the surrounding topology. By specifying to DM the topology that is appropriate for your networking application, DM can present more relevant options and guidance.

The network topology is often determined solely by your existing network; however, the goals for your ACE deployment can also play a role. For example, when ACE acts as a router between clients and servers, it provides a level of protection by effectively hiding the servers from the clients. On the other hand, for a routed topology to work, each of those servers must be configured to route back through the ACE, which can be a significant change to the network routing.

The ACE is also capable of bridging the client and server VLANs, which does not affect server routing. However, it does require the network to have VLANs set up appropriately.

If you are not sure what topology to use, or do not want to make topology decisions immediately, use the “one-armed” topology. The one-armed topology does not typically require any changes to an existing network and can be set up with minimal knowledge of the network. You can then expand your ACE network topology to routed mode or bridged mode to better suit your networking requirements.

[Figure 3-1](#) illustrates the one-armed network topology.

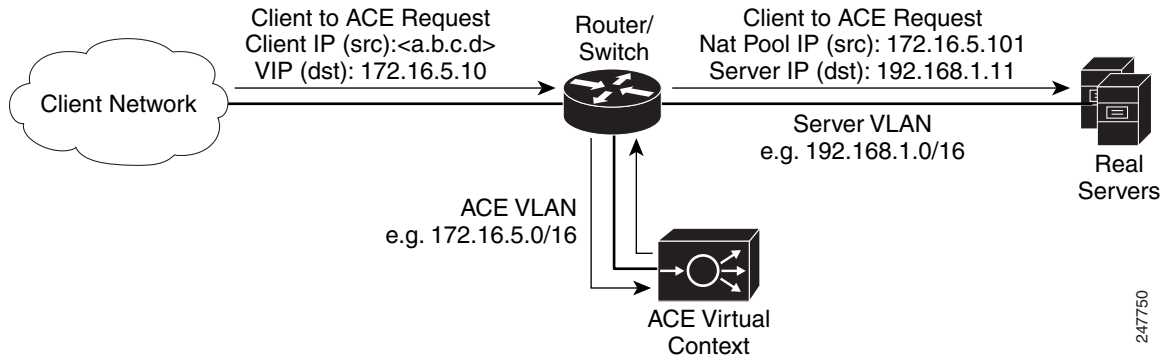
Figure 3-1 Example of a One-Armed Network Topology

Figure 3-2 illustrates the routed mode network topology.

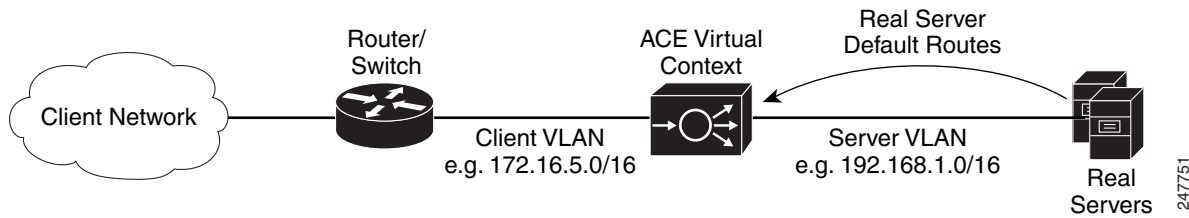
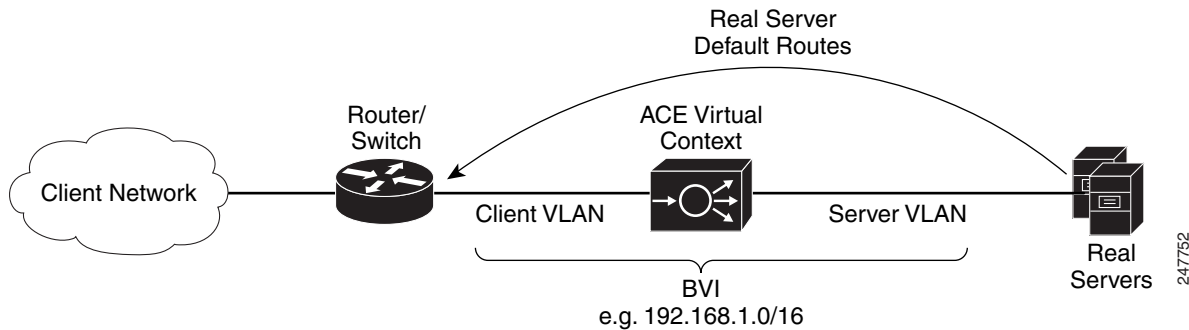
Figure 3-2 Example of a Routed Mode Network Topology

Figure 3-3 illustrates the bridged mode network topology.

Figure 3-3 Example of a Bridged Mode Network Topology

Using Application Setup

You use the Application Setup task to set up load balancing for an application.

Procedure

Step 1 Choose **Config > Guided Setup > Application Setup**.

The Application Setup window appears.

- Step 2** From the Select Virtual Context drop-down list, choose an existing ACE virtual context.
- Step 3** If your ACE is to use HTTPS when communicating with either the client or with real servers, in the Use HTTPS (SSL) field, choose **Yes** to specify that the ACE should be set up for secure (SSL) Hypertext Transfer Protocol (HTTP).



Note The HTTPS option does not apply to the ACE NPE software version. The radio button is set to No and cannot be changed. For more information, see the [“Information About the ACE No Payload Encryption Software Version” section on page 1-2](#).

- Step 4** Choose the network topology that reflects the relationship of the selected ACE virtual context to the real servers in the network.
- Topology choices include one-armed, routed, or bridged. See the [“ACE Network Topology Overview” section on page 3-9](#) for background details on networking topology.

- Step 5** Click **Start Setup**.

- Step 6** If you selected either the one-armed or routed topology, the VLAN Interfaces window appears (Config > Guided Setup > Application Setup > VLAN Interfaces).

To communicate with the client and real servers, a VLAN interface must be specified for client and server traffic to be sent and received.

Perform the following actions to configure a VLAN interface:

- a. Click **Add** to add a new VLAN interface, or choose an existing VLAN interface and click **Edit** to modify it.
- b. Enter the VLAN interface attributes as described in the [“Configuring Virtual Context VLAN Interfaces” section on page 10-10](#). Click **More Settings** to access the additional VLAN interface attributes. By default, DM hides the default VLAN interface attributes and the VLAN interface attributes which are not commonly used.



Note After you define the VLAN, write down the VLAN number. You will need this VLAN number in the ACL and virtual server steps (Steps 9 and 11) of this procedure.

- c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
 - d. To display statistics and status information for a VLAN interface, choose the VLAN interface from the VLAN Interface table, and then click **Details**. The **show interface vlan**, **show ipv6 interface vlan**, and **show ipv6 neighbors** CLI commands appear. Click on the command to display its output. See the [“Displaying VLAN Interface Statistics and Status Information” section on page 10-23](#) for details.
- Step 7** If you selected the bridged topology, the BVI Interfaces window appears (Config > Guided Setup > Application Setup > BVI Interfaces).

Perform the following actions to configure a BVI interface:

- a. Click **Add** to add a new BVI interface, or choose an existing BVI interface, and then click **Edit** to modify it.
- b. Enter the BVI interface attributes as described in the [“Configuring Virtual Context BVI Interfaces” section on page 10-23](#).

**Note**

After you define the BVI, write down the client-side VLAN number. You will need this BVI number in the ACL and virtual server steps (Steps 9 and 11) of this procedure.

- c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
- d. To display statistics and status information for a BVI interface, choose the BVI interface from the BVI Interface table, and then click **Details**. The **show interface bvi**, **show ipv6 interface bvi**, and **show ipv6 neighbors** CLI commands appear. Click on the command to display its output. See the [“Displaying BVI Interface Statistics and Status Information” section on page 10-31](#) for details.

Step 8 If you selected the one-armed topology, click **NAT Pools** under Application Setup.

The NAT Pools window appears (Config > Guided Setup > Application Setup > NAT Pools). To set up a one-armed topology, you need a NAT pool to provide the set of IP addresses that ACE can use as source addresses when sending requests to the real servers.

**Note**

You must configure the NAT pool on the same VLAN interface that you configured in Step 6.

Perform the following actions to create or modify a NAT pool for a VLAN:

- a. Click **Add** to add a new NAT pool entry, or choose an existing NAT pool entry and click **Edit** to modify it. The NAT Pool configuration window appears.
- b. Configure the NAT pool attributes as described in the [“Configuring VLAN Interface NAT Pools and Displaying NAT Utilization” section on page 10-32](#).

**Note**

After you define the NAT pool, write down the NAT pool ID. You will specify the NAT pool ID in the virtual server step (Step 11) of this procedure.

- c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Step 9 Click **ACLs** under Application Setup.

The ACLs window appears (Config > Guided Setup > Application Setup > ACLs). An ACL applies to one or more VLAN interfaces. Each ACL consists of a list of entries, each of which defines a source, a destination, and whether to permit or deny traffic between those locations.

Perform the following actions to create or modify an ACL:

- a. Click **Add** to add a new ACL entry, or choose an existing ACL entry and click **Edit** to modify it. The Access List configuration window appears.
- b. Add or edit the required fields as described in the [“Configuring Security with ACLs” section on page 4-58](#).
- c. Click **Deploy** to save this configuration.
- d. To display statistics and status information for an ACL, choose an ACL from the ACLs table, and then click **Details**. The **show access-list access-list detail** CLI command output appears. See the [“Displaying ACL Information and Statistics” section on page 4-69](#) for details.

Step 10 Click **SSL Proxy** under Application Setup.

This selection appears only if you specified in Step 3 that the ACE is to use HTTPS when communicating with either the client or with real servers.

The SSL Proxy window appears (Config > Guided Setup > Application Setup > SSL Proxy).



Note To terminate or initiate HTTPS connections with ACE, the virtual context must have at least one SSL proxy service. An SSL proxy contains the certificate and key information needed to terminate HTTPS connections from the client or initiate them to the servers.

Perform the following actions to create or modify an SSL proxy service:

- a. To create an SSL proxy service, click **SSL Proxy Setup**.



Note To edit an existing SSL proxy service, choose it from the SSL Proxy table, and click **Edit** to modify the SSL proxy service. The SSL Proxy Service configuration window appears. Edit the required fields as described in the “[Configuring SSL Proxy Service](#)” section on [page 9-28](#).

- b. Add required fields as described in the “[Configuring SSL Proxy Service](#)” section on [page 9-28](#).
- c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.

Step 11 Click **Virtual Server** under Application Setup.

The Virtual Servers window appears (Config > Guided Setup > Application Setup > Virtual Server). The virtual server defines the load-balancing configuration for an application.

Perform the following actions to create or modify a virtual server:

- a. Click **Add** to add a new virtual server, or choose an existing virtual server, and click **Edit** to modify it. The Virtual Server configuration window appears with a number of configuration subsets. The subsets that you see depend on whether you use the Basic View or the Advanced View and entries you make in the Properties subset. Change views by using the View object selector at the top of the configuration pane.
- b. Add or edit required fields as described in the “[Virtual Server Configuration Procedure](#)” section on [page 5-7](#). [Table 5-1](#) identifies and describes virtual server configuration subsets with links to related topics for configuration information.

Virtual servers have many configuration options. At a minimum, you need to configure the following attributes:

- Set the VIP, port number (TCP or UDP), and application protocol for your application.



Note If the ACE is to terminate the client HTTPS connections, choose **HTTPS** as the Application Protocol.

- (One-Armed Topology) For VLAN, choose the VLAN from Step 6.
- (Routed Topology) For VLAN, choose the client-side VLAN from Step 6.
- (Bridged Topology) For VLAN, choose the client-side VLAN from Step 6.
- If the ACE is to terminate client HTTPS connections, then under the SSL Termination header, specify the SSL proxy defined in Step 10.
- Under the Default L7 Loadbalancing Action, set Primary Action to **Loadbalance**.

- Create a server farm that contains one or more real servers for this application (see [Table 5-10](#) in the “[Configuring Virtual Server Layer 7 Load Balancing](#)” section for details on setting server farm attributes).
- If the ACE is to initiate HTTPS connections to the real servers, choose the desired SSL proxy for initiation to this application from the menu next to SSL Initiation.
- (One-Armed Topology) Under NAT, enter the NAT pool ID from Step 8.

After you set up a base virtual server, you can test it to validate your configuration and isolate any issues in your networking application. You can then add these more advanced load balancing options to your networking application:

- Additional real servers to a server farm. See [Table 5-10](#) in the “[Configuring Virtual Server Layer 7 Load Balancing](#)” section for details.
 - Health monitoring probes and attributes for the specific probe type. See [Table 5-11](#) in the “[Configuring Virtual Server Layer 7 Load Balancing](#)” section for details.
 - Stickiness, where client requests for content are to be handled by a sticky group when match conditions are met. See [Table 5-13](#) in the “[Configuring Virtual Server Layer 7 Load Balancing](#)” section for details.
 - Application protocol inspection, where the ACE allows the virtual server to verify protocol behavior and identify unwanted or malicious traffic passing through the ACE. See the “[Configuring Virtual Server Protocol Inspection](#)” section for details.
- c. Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
 - d. To display statistics and status information for an existing virtual server, choose a virtual server from the Virtual Servers table, and then click **Details**. The **show service-policy global detail** CLI command output appears. See the [Viewing All Virtual Servers, page 5-65](#) for details.

Related Topics

- [Using ACE Hardware Setup, page 3-3](#)
- [Using Virtual Context Setup, page 3-7](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context BVI Interfaces, page 10-23](#)
- [Configuring Virtual Context Static Routes, page 10-34](#)
- [Configuring Security with ACLs, page 4-58](#)
- [SSL Setup Sequence, page 9-5](#)



CHAPTER 4

Configuring Virtual Contexts

Cisco Application Control Engine Appliance Device Manager (ACE Appliance Device Manager) provides a number of options for creating, configuring, and managing ACE appliances.



Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

This chapter contains the following sections:

- [Using Virtual Contexts, page 4-2](#)
- [Creating Virtual Contexts, page 4-2](#)
- [Configuring Virtual Contexts, page 4-7](#)
- [Configuring Virtual Context System Attributes, page 4-11](#)
- [Configuring Virtual Context Primary Attributes, page 4-11](#)
- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring SNMP for Virtual Contexts, page 4-19](#)
- [Configuring Virtual Context Global Traffic Policies, page 4-28](#)
- [Managing ACE Appliance Licenses, page 4-29](#)
- [Managing Resource Classes, page 4-35](#)
- [Setting Resource Usage Thresholds to Receive SNMP Notifications, page 4-42](#)
- [Using the Configuration Checkpoint and Rollback Service, page 4-46](#)
- [Performing Device Backup and Restore Functions, page 4-49](#)
- [Configuring Security with ACLs, page 4-58](#)
- [Configuring Object Groups, page 4-70](#)
- [Configuring Virtual Context Expert Options, page 4-79](#)
- [Managing Virtual Contexts, page 4-79](#)

Using Virtual Contexts

Virtual contexts use the concept of virtualization to partition your ACE appliance into multiple virtual devices or contexts. Each context contains its own set of policies, interfaces, resources, and administrators. This feature enables you to more closely and efficiently manage resources, users, and the services you provide to your customers.

The first time you configure a virtual context, you will see only the Admin context. In addition to the configurable attributes of other virtual contexts, the Admin context can configure:

- ACE appliance licenses
- Resource classes
- Port channel, management, and Gigabit Ethernet interfaces
- High Availability (HA or fault tolerance between ACE appliances)
- Application acceleration and optimization on the ACE appliance

Related Topics

- [Creating Virtual Contexts, page 4-2](#)
- [Configuring Virtual Contexts, page 4-7](#)
- [Deleting Virtual Contexts, page 4-84](#)

Creating Virtual Contexts

Use this procedure to create virtual contexts.



Note

If you do not configure a management VLAN for SNMP access, the ACE Appliance Device Manager will not be able to poll the context.



Note

If an ACE appliance is configured as a hot standby in a high availability pair, its configuration cannot be modified and you cannot add or modify virtual contexts. ACE appliances configured as hot standby members display *Standby Hot* in the HA State column in the All Virtual Contexts table (**Config > Virtual Contexts**). For more information, see the “[High Availability Polling](#)” section on page 11-2.

Procedure

- Step 1** Choose **Config > Virtual Contexts**.
The All Virtual Contexts table appears.
- Step 2** Click **Add**.
The New Virtual Context screen appears.
- Step 3** Configure the virtual context using the information in [Table 4-1](#).



Tip

Fields with 2 or 3 choices use radio buttons. Fields with more than 3 choices use dropdown lists.

Table 4-1 Virtual Context Configuration Attributes

Field	Description
Basic Settings	
Name	Enter a unique name for the virtual context. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. This field is read-only for existing contexts.
Description	Enter a brief description of the virtual context. Enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.
Resource Class	Choose the resource class this virtual context is to use. Click View to display the information for the selected resource class. For more information, see the “Managing Resource Classes” section on page 4-35).
Allocate VLANs	Enter the number of a VLAN or a range of VLANs so that the context can receive the associated traffic. You can specify VLANs in any of the following ways: <ul style="list-style-type: none"> For a single VLAN, enter an integer from 2 to 4096. For multiple, non-sequential VLANs, use comma-separated entries, such as 101, 201, 302. For a range of VLANs, use the format <i><beginning-VLAN>-<ending-VLAN></i>, such as 101-150. Note VLANs cannot be modified in an Admin context.
Default Gateway for IPv4	Enter the IPv4 address of the default gateway. You can enter a maximum of eight addresses. Use a comma-separated list to specify multiple IP addresses, for example, such as 192.168.65.1, 192.168.64.2. Default static routes with a netmask and IP address of 0.0.0.0 previously configured on the ACE appear in this field.
Default Gateway for IPv6	Enter the IPv6 address of the default gateway or select the forward VLAN interface or BVI, as follows: <ul style="list-style-type: none"> IPv6 Address field—Enter the address of the gateway router (the next-hop address for this route). Then, use the right arrow to move it to the Selected field. You can enter a maximum of eight addresses including a selected VLAN or BVI through the Outgoing Interfaces setting. Default static routes with a prefix and IP address of ::0 previously configured on the ACE appear in the Selected field. Outgoing Interfaces—Select either VLAN or BVI used for the link-local address only. And then select the Interface Number for the VLAN or BVI.
Management Settings	
VLAN Id	Enter the VLAN number that you want to assign to the management interface. Valid values are from 2 to 4094. By default, all devices are assigned to VLAN1, known as the default VLAN. The ACE Device Manager identifies the management class maps and policy maps associated with the selected VLAN ID assigned to the management interface. This field is read-only if configured for existing contexts.
VLAN Description	Enter a description for the management interface. Enter an unquoted text string that contains a maximum of 240 alphanumeric characters including spaces.

Table 4-1 Virtual Context Configuration Attributes (continued)

Field	Description
Interface Mode	<p>Choose the topology that reflects the relationship of the selected ACE virtual context to the real servers in the network:</p> <ul style="list-style-type: none"> • Routed—The ACE virtual context acts as a router between the client-side network and the server-side network. In this topology, every real server for the application must be routed through the ACE virtual context, either by setting the default gateway on each real server to the virtual context server-side VLAN interface address, or by using a separate router with appropriate routes configured between the ACE virtual context and the real servers. • Bridged—The virtual ACE bridges two VLANs—a client-side VLAN and a real-server VLAN—on the same subnet using a bridged virtual interface (BVI). In this case, the real server routing does not change to accommodate the ACE virtual context. Instead, the virtual ACE transparently handles traffic to and from the real servers. <p>This field is read-only if configured for existing contexts.</p>
Management IP	<p>Enter the IPv4 address that is to be used for remote management of the context. This address must be a unique management IP address that is not used in another context. The DM does not support duplicate management IP addresses in different contexts.</p> <p>Note The Device Manager considers an interface as a management interface if it has a management policy map associated with the VLAN interface. See the “Configuring Virtual Context VLAN Interfaces” section on page 10-10.</p>
Management Netmask	Choose the subnet mask to apply to this IP address.
Alias IP Address	Enter the IPv4 address of the alias associated with this interface.
Peer IP Address	Enter the IPv4 address of the remote peer.
Access Permission	<p>Choose the source IP addresses that are allowed on the management interface as follows:</p> <ul style="list-style-type: none"> • Allow All—Allows all configured client source IP addresses on the management interface as the network traffic matching criteria. • Deny All—Denies all configured client source IP addresses on the management interface as the network traffic matching criteria. • Match—Displays the Match Conditions table, where you specify the match criteria that the ACE is to use for traffic on the management interface.

Table 4-1 Virtual Context Configuration Attributes (continued)


Field	Description
Match Conditions	<p>When you enter the VLAN ID for the management interface, the Match Conditions table appears.</p> <p>To add or modify the protocols allowed on this management VLAN, do the following:</p> <ol style="list-style-type: none"> Click Add to choose a protocol for the management interface, or choose an existing protocol entry listed in the Match Conditions table and click Edit to modify it. In the Protocol drop-down list, choose a protocol: <ul style="list-style-type: none"> HTTP—Specifies the Hypertext Transfer Protocol (HTTP). HTTPS—Specifies the Hypertext Transfer Protocol Secure (HTTPS) for connectivity with the interface using port 443. ICMP—Specifies the Internet Control Message Protocol (ICMP) for Internet Protocol version 4 (IPv4). ICMPv6—Specifies the Internet Control Message Protocol version 6 (ICMPv6) for Internet Protocol version 6 (IPv6). KALAP-UDP—Specifies the Keepalive Appliance Protocol over UDP. SNMP—Specifies the Simple Network Management Protocol (SNMP). <p> Note If SNMP is not selected, the ACE Appliance Device Manager cannot poll the context.</p> <ul style="list-style-type: none"> SSH—Specifies a Secure Shell (SSH) connection to the ACE. TELNET—Specifies a Telnet connection to the ACE. XML-HTTPS—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS) using port 10443. This option is available for ACE appliances only. <ol style="list-style-type: none"> In the Allowed From field, specify the matching criteria for the client source IP address: <ul style="list-style-type: none"> Any—Specifies any client source address for the management traffic classification. Source Address—Specifies a client source host IP address as the network traffic matching criteria. An ICMPv6 source address only accept an IPv6 address. Source Netmask—Select a subnet mask. This field is not applicable for ICMPv6. Source Prefix Length—(ICMPv6 only) Enter the prefix length, a value from 1 to 128. Click OK to accept the protocol selection or click Cancel to exit without accepting your entries. <p>Note To remove a protocol from the management VLAN, choose the entry in the Match Conditions table, and click Delete.</p>
Enable SNMP Get	<p>Check this check box to add an SNMP Get community string to enable SNMP polling on this context.</p> <p>This field is read-only if configured for existing contexts.</p>

Table 4-1 Virtual Context Configuration Attributes (continued)

Field	Description
SNMP v2c Read-Only Community String	<p>When you check the Enable SNMP Get check box, this field appears.</p> <p>Enter the SNMPv2c read-only community string to be used as the SNMP Get community string.</p> <p>This field is read-only if configured for existing contexts.</p> <p>Note If SNMP is not an allowed protocol, the ACE Appliance Device Manager will not be able to poll the context.</p>
Add Admin User	When initially configuring the context, check this check box to configure this context for an Admin user. When the fields appear, enter the user name and password, and confirm the password.
More Settings	
Switch Mode	<p>Check this check box to change the way that the ACE processes TCP connections that are not destined to a VIP or that do not have any policies associated with their traffic. For such traffic, the ACE still creates connection objects but processes the connections as stateless connections, which means that they do not undergo any TCP normalization checks. With this option enabled, the ACE also creates stateless connections for non-SYN TCP packets if they satisfy all other configured requirements. This process ensures that a long-lived persistent connection passes through the ACE successfully (even if it times out) by being reestablished by any incoming packet related to the connection.</p> <p>By default, these stateless connections time out after 2 hours and 15 minutes unless you configure the inactivity timeout otherwise in a parameter map. When a stateless connection times out, the ACE does not send a TCP RST packet but silently closes the connection. Even though these connections are stateless, the TCP RST and FIN-ACK flags are honored and the connections are closed when the ACE sees these flags in the received packets.</p>
Shared VLAN Host Id	Specific bank of MAC addresses that the ACE uses. Enter a number from 1 to 16. Be sure to configure different bank numbers for multiple ACEs. This field is available only in the Admin context.
Regex Compilation Timeout (minutes)	Enter the timeout for regex compilation in minutes. When you configure a regex and its compilation is longer than the configured timeout, the ACE stops the regex compilation. A valid entry is an integer from 1 to 500. The default timeout is 60. This field is available only in the Admin context.

Step 4 Do one of the following

- Click **Deploy Now** to deploy this virtual context. To configure other virtual context attributes, see the [“Configuring Virtual Contexts” section on page 4-7](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the All Virtual Contexts table.

Related Topics

- [Using Virtual Contexts, page 4-2](#)
- [Configuring Virtual Contexts, page 4-7](#)

Configuring Virtual Contexts

After creating a virtual context, you can configure it. Configuring a virtual context involves configuring a number of attributes, grouped into *configuration subsets*. [Table 4-2](#) describes ACE Appliance Device Manager configuration subsets and provides links to related topics.

**Note**

If an ACE appliance is configured as a hot standby in a high availability pair, its configuration cannot be modified and you cannot add or modify virtual contexts. ACE appliances configured as hot standby members display *Standby Hot* in the HA State column in the All Virtual Contexts table (**Config > Virtual Contexts**). For more information, see the [“High Availability Polling” section on page 11-2](#).

**Note**

To add objects such as real servers or server farms to a customized domain, use the CLI and then use the synchronize feature in ACE Appliance Device Manager to add this object into its customized domain on ACE Appliance Device Manager. Adding objects to customized domains directly in ACE Appliance Device Manager results in the object being added to the default domain.

Synchronization options are available in the All Virtual Contexts table (**Config > Virtual Contexts**).

**Tip**

Fields with 2 or 3 choices use radio buttons. Fields with more than 3 choices use dropdown lists.

Table 4-2 ACE Appliance and Virtual Context Configuration Options

Configuration Subset	Description	Related Topics
System	<p>System configuration options allow you to configure:</p> <ul style="list-style-type: none"> Primary attributes such as VLANs, SNMP access, and resource class. Syslog attributes including the type and severity of syslog messages that are to be logged, the syslog log host, log messages, and log rate limits. SNMP attributes. Global policy map configuration for all VLANs on a virtual context. ACE license use on the ACE appliance. Resource classes for allocation of ACE appliance resources. Application acceleration and optimization on the ACE appliance. Checkpoint (snapshot in time) of a known stable running configuration. Back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context. <p>Note ACE appliance licenses, resource classes, and acceleration and optimization can be configured only in an Admin context.</p>	<ul style="list-style-type: none"> Configuring Virtual Context Primary Attributes, page 4-11 Configuring Virtual Context Syslog Logging, page 4-12 Configuring SNMP for Virtual Contexts, page 4-19 Configuring Virtual Context Global Traffic Policies, page 4-28 Managing ACE Appliance Licenses, page 4-29 Managing Resource Classes, page 4-35 Configuring Global Application Acceleration and Optimization, page 13-9 Using the Configuration Checkpoint and Rollback Service, page 4-46 Performing Device Backup and Restore Functions, page 4-49

Table 4-2 ACE Appliance and Virtual Context Configuration Options (continued)

Configuration Subset	Description	Related Topics
Load Balancing	<p>Load-balancing attributes allow you to:</p> <ul style="list-style-type: none"> • Configure virtual servers, real servers, and server farms for load balancing. • Establish the predictor method and return code checking. • Implement sticky groups for session persistence. • Configure parameter maps to combine related actions for policy maps. <p>Load-balancing configuration options include:</p> <ul style="list-style-type: none"> • Virtual servers • Real servers • Server farms • Health monitoring • Sticky attributes • Parameter maps • Secure KAL-AP • Dynamic Workload Scaling (admin context only) 	<ul style="list-style-type: none"> • Load Balancing Overview, page 5-1 • Configuring Virtual Servers, page 5-2 • Configuring Server Farms, page 6-18 • Configuring Health Monitoring for Real Servers, page 6-41 • Configuring Sticky Groups, page 7-11 • Configuring Parameter Maps, page 8-1 • Configuring Secure KAL-AP, page 6-70 • Configuring Dynamic Workload Scaling, page 6-14
SSL	<p>SSL configuration options allow you to:</p> <ul style="list-style-type: none"> • Import and export SSL certificates and keys. • Set up SSL parameter maps and chain group parameters. • Generate certificate signing requests for submission to a certificate authority. • Authenticate peer certificates. • Configure certificate revocation lists for use during client authentication. • Configure an Online Certificate Status Protocol (OCSP) service to define the host server for certificate revocation checks using OCSP. 	<ul style="list-style-type: none"> • Configuring SSL, page 9-1 • Using SSL Certificates, page 9-6 • Using SSL Keys, page 9-11 • Generating CSRs, page 9-27 • Configuring SSL Parameter Maps, page 9-19 • Configuring SSL Chain Group Parameters, page 9-25 • Configuring SSL Proxy Service, page 9-28 • Configuring SSL Authentication Groups, page 9-32 • Configuring SSL OCSP Service, page 9-30 • Configuring CRLs for Client Authentication, page 9-33
Security	<p>Security configuration options allow you to create access control lists, set ACL attributes, resequence ACLs, delete ACLs, and configure object groups.</p>	<ul style="list-style-type: none"> • Configuring Virtual Context Expert Options, page 4-79 • Creating ACLs, page 4-59 • Configuring Object Groups, page 4-70

Table 4-2 ACE Appliance and Virtual Context Configuration Options (continued)

Configuration Subset	Description	Related Topics
Network	<p>Network configuration options allow you to configure:</p> <ul style="list-style-type: none"> • Port channel interfaces • Gigabit Ethernet interfaces • VLAN interfaces • BVI interfaces • Network Address Translation (NAT) pools for a VLAN interface • Static routes • DHCP relay agents <p>Note You can configure port channel and Gigabit Ethernet interfaces only in an Admin context.</p>	<ul style="list-style-type: none"> • Configuring Virtual Context BVI Interfaces, page 10-23 • Configuring Gigabit Ethernet Interfaces, page 10-5 • Configuring Virtual Context VLAN Interfaces, page 10-10 • Configuring Virtual Context BVI Interfaces, page 10-23 • Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32 • Configuring Virtual Context Static Routes, page 10-34 • Configuring Global IP DHCP, page 10-35
High Availability	<p>High Availability (HA) attributes allow you to configure two ACE appliances for fault-tolerant redundancy.</p> <p>Note You can set up high availability only in an Admin virtual context.</p>	<ul style="list-style-type: none"> • Configuring High Availability, page 11-1 • Configuring High Availability Peers, page 11-8 • Configuring ACE High Availability Groups, page 11-11
HA Tracking And Failure Detection	<p>HA Tracking And Failure Detection attributes allow you to configure tracking processes that can help ensure reliable fault tolerance.</p>	<ul style="list-style-type: none"> • High Availability Tracking and Failure Detection Overview, page 11-17 • Tracking VLAN Interfaces for High Availability, page 11-19 • Tracking Hosts for High Availability, page 11-20
Expert	<p>Expert options allow you to:</p> <ul style="list-style-type: none"> • Configure traffic policies for filtering and handling traffic received by or passing through the ACE appliance. • Configure optimization action lists. • Configure HTTP header modify action lists. 	<ul style="list-style-type: none"> • Configuring Traffic Policies, page 12-1 • Configuring an HTTP Optimization Action List, page 13-3 • Configuring an HTTP Header Modify Action List, page 12-90

Configuring Virtual Context System Attributes

Table 4-3 identifies the ACE Appliance Device Manager virtual context System configuration options and related topics for more information.

Table 4-3 *Virtual Context System Configuration Options*

System Configuration Options	Related Topics
Specify virtual context primary attributes	Configuring Virtual Context Primary Attributes, page 4-11
Configure syslog options	<ul style="list-style-type: none"> • Configuring Virtual Context Syslog Logging, page 4-12 • Configuring Syslog Log Hosts, page 4-16 • Configuring Syslog Log Messages, page 4-17 • Configuring Syslog Log Rate Limits, page 4-18
Configure SNMP attributes	<ul style="list-style-type: none"> • Configuring SNMP for Virtual Contexts, page 4-19 • Configuring SNMP Version 2c Communities, page 4-20 • Configuring SNMP Version 3 Users, page 4-21 • Configuring SNMP Trap Destination Hosts, page 4-23 • Configuring SNMP Notifications, page 4-25
Establish global policy maps for all VLANs on a virtual context	Configuring Virtual Context Global Traffic Policies, page 4-28
Manage ACE appliance licenses	Managing ACE Appliance Licenses, page 4-29
Manage ACE appliance resources across virtual contexts	Managing Resource Classes, page 4-35
Establish application acceleration and optimization for the ACE appliance	Configuring Global Application Acceleration and Optimization, page 13-9
Back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context	Performing Device Backup and Restore Functions, page 4-49

Configuring Virtual Context Primary Attributes

Primary attributes specify a name and resource class for each virtual context. After providing this information, you can configure other attributes, such as interfaces, monitoring, or load-balancing. For a complete list of configuration options, see the “[Configuring Virtual Contexts](#)” section on page 4-7.

Use this procedure to configure virtual context primary attributes.

Procedure

-
- Step 1** Choose **Config > Virtual Contexts > context > System > Primary Attributes**.
The Primary Attributes configuration screen appears.
- Step 2** Enter the primary attributes for this virtual context as described in [Table 4-1](#).
- Step 3** Click **Deploy Now** to deploy this configuration on the ACE appliance.
To exit this procedure without accepting your entries, select a different configuration option.
-

Related Topics

- [Using Virtual Contexts, page 4-2](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context BVI Interfaces, page 10-23](#)
- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring Traffic Policies, page 12-1](#)

Configuring Virtual Context Syslog Logging

The ACE Appliance Device Manager uses syslog logging to send log messages to a process which logs messages to designated locations asynchronously to the processes that generated the messages.

Procedure

-
- Step 1** Choose **Config > Virtual Contexts > context > System > Syslog**.
The Syslog configuration screen appears.
- Step 2** Enter the syslog logging attributes in the displayed fields (see [Table 4-5](#)).
All fields that require you to select syslog severity levels use the values in [Table 4-4](#).

Table 4-4 Syslog Logging Levels

Severity	Description
0-Emergency	Unusable system
1-Critical	Critical condition
2-Warning	Warning condition
3-Alert	Immediate action required
4-Error	Error condition
5-Notification	Normal but significant condition
6-Information	Informational message only
7-Debug	Appears only during debugging

The severity level that you specify indicates that you want syslog messages at that level and the more severe levels. For example, if you specify Error, syslog displays Error, Critical, Alert, and Emergency messages.



Note If you set all syslog levels to Debug, some commands like **switchover** are not processed successfully. These commands are issued via the CLI and ACE Appliance Device Manager cannot parse the returned prompt if Debug level is enabled. Instead, a timeout message is displayed.

If you set syslog levels to Debug and then issue a command that results in a timeout message, click **Refresh** to view the result of the operation.



Note Setting all syslog levels to Debug during normal operation can degrade overall performance.

Table 4-5 Virtual Context Syslog Configuration Attributes

Field	Description	Action
Enable Syslog	This option indicates whether syslog logging should be enabled or disabled.	Check the check box to enable syslog logging or clear the check box to disable syslog logging.
Facility	The syslog daemon uses the specified syslog facility to determine how to process the messages it receives. Syslog servers file or direct messages based on the facility number in the message. For more information on the syslog daemon and facility levels, refer to your syslog daemon documentation.	Enter the facility appropriate for your network. Valid entries are 16 (LOCAL0) through 23 (LOCAL7). The default for an ACE appliance is 20 (LOCAL4).
Buffered Level	This option enables system logging to a local buffer and limits the messages sent to the buffer based on severity.	Choose the desired level for sending system log messages to a local buffer. This option is disabled by default.
Console Level	This option specifies the maximum level for system log messages sent to the console.	Select the desired level for sending system log messages to the console. This option is disabled by default. Note Logging into the console can degrade system performance. Therefore, we recommend that you log messages to the console only when you are testing or debugging problems. Do not use this option when the network is busy, as it can reduce ACE appliance performance.

Table 4-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
History Level	This option specifies the maximum level for system log messages sent as traps to an SNMP network management station.	<p>Choose the desired level for sending system log messages as traps to an SNMP network management station.</p> <p>This option is disabled by default.</p> <p>Note For more information about configuring SNMP, see the “Configuring SNMP Notifications” section on page 4-25.</p>
Monitor Level	This option specifies the maximum level for system log messages sent to a remote connection using Secure Shell (SSH) or Telnet on the ACE appliance.	<p>Select the desired level for sending system log messages to a remote connection using SSH or Telnet on the ACE appliance.</p> <p>This option is disabled by default.</p> <p>Note You must enable remote access on the ACE appliance and establish a remote connection using the SSH or Telnet protocol from a PC for this option to work.</p>
Persistence Level	This option specifies the maximum level for system log messages sent to Flash memory.	<p>Select the desired level for sending system log messages to Flash memory.</p> <p>This option is disabled by default.</p> <p>Note We recommend that you use a lower severity level, such as 3, since logging at a high rate to Flash memory on the ACE appliance might impact performance.</p>
Trap Level	This option specifies the maximum level for system log messages sent to a syslog server.	<p>Select the desired level for sending system log messages to a syslog server.</p> <p>This option is disabled by default.</p>
Queue Size	This option specifies the size of the buffer for storing syslog messages received from other processes within the ACE appliance while they await processing. When the queue exceeds the specified value, the excess messages are discarded.	<p>Enter the desired queue size.</p> <p>Valid entries are from 0 to 8192 messages.</p> <p>The default is 100 messages.</p>
Enable Timestamp	This option indicates whether syslog messages should include the date and time that the message was generated.	<p>Check the check box to enable timestamps on syslog messages or clear the check box to disable timestamps on syslog messages.</p> <p>This option is disabled by default.</p>
Enable Standby	<p>This option indicates whether logging is enabled on the failover standby ACE appliance. When enabled:</p> <ul style="list-style-type: none"> • This feature causes twice the message traffic on the syslog server. • The standby ACE appliance syslog messages remain synchronized if failover occurs. 	<p>Check the check box to enable logging on the failover standby ACE appliance or clear the check box to disable logging on the failover standby ACE appliance.</p>

Table 4-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Enable Fastpath Logging	This option indicates whether connection setup and teardown messages are logged.	Check the check box to enable the logging of setup and teardown messages or clear the check box to disable the logging of setup and teardown messages. This option is disabled by default.
Device Id Type	This option specifies the type of unique device identifier to be included in syslog messages sent to the syslog server. The device identifier does not appear in EMBLEM-formatted messages, SNMP traps, or on the ACE appliance console, management session, or buffer.	Select the type of device identifier to be used: <ul style="list-style-type: none"> Any String—Indicates that a test string is to be used to uniquely identify syslog messages sent from the ACE appliance. Context Name—Indicates that the name of the current virtual context is to be used to uniquely identify the syslog messages sent from the ACE appliance. Host Name—Indicates that the hostname of the ACE appliance is to be used to uniquely identify the syslog messages sent from the ACE appliance. Interface—Indicates that the IP address of the interface is to be used to uniquely identify the syslog messages sent from the ACE appliance. Undefined—Indicates that no identifier is to be used.
Device Interface Name	This field appears if the Device Id Type is Interface. This option specifies the logging device interface to be used to uniquely identify syslog messages sent from the ACE appliance.	Enter a text string that uniquely identifies the logging device interface name whose ID is to be included in system messages. The maximum string length is 64 characters without spaces. Do not use the following characters: & (ampersand), ' (single quote), " (double quote), < (less than), > (greater than), or ? (question mark).
Logging Device Id	This field appears if the Device ID Type is Any String. This option specifies the text string to be used to uniquely identify syslog messages sent from the ACE appliance.	Enter a text string that uniquely identifies the syslog messages sent from the ACE appliance. The maximum string length is 64 characters without spaces. Do not use the following characters: & (ampersand), ' (single quote), " (double quote), < (less than), > (greater than), or ? (question mark).

Step 3 Click **Deploy Now** to deploy this configuration on the ACE appliance.

To configure other Syslog attributes for this virtual context, see the following topics:

- [Configuring Syslog Log Hosts, page 4-16](#)
- [Configuring Syslog Log Messages, page 4-17](#)
- [Configuring Syslog Log Rate Limits, page 4-18](#)

Related Topics

- [Configuring Virtual Contexts, page 4-7](#)

- [Configuring Syslog Log Hosts, page 4-16](#)
- [Configuring Syslog Log Messages, page 4-17](#)
- [Configuring Syslog Log Rate Limits, page 4-18](#)

Configuring Syslog Log Hosts

After configuring basic syslog characteristics (see the “[Configuring Virtual Context Syslog Logging](#)” section on [page 4-12](#)), you can configure the log host, log messages, and log rate limits. The tabs for these attributes appear beneath the Syslog configuration screen.

Guidelines and Restrictions

You can configure the ACE with a maximum of four log hosts per context.

Procedure

-
- Step 1** Choose **Config > Virtual Contexts > context > System > Syslog**.
The Syslog configuration screen appears.
 - Step 2** Select the **Log Host** tab.
The Log Host table appears.
 - Step 3** Click **Add** to add a new log host, or select an existing log host, and then click **Edit** to modify it.
The Log Host configuration screen appears.
 - Step 4** In the IP Address field, enter the IPv4 address of the host to be used as the syslog server.
 - Step 5** In the Protocol field, select TCP or UDP as the protocol to be used.
 - Step 6** In the Protocol Port field, enter the number of the port that the syslog server listens to for syslog messages.
Valid entries are from 1 to 65535. The default port for TCP is 1470 and for UDP it is 514.
 - Step 7** If it is present, check the **Default UDP** check box to specify that the ACE appliance is to default to UDP if the TCP transport fails to communicate with the syslog server.
The Default UDP check box appears if TCP is selected in the Protocol field ([Step 5](#)). Clear this check box to prevent the ACE appliance from defaulting to UDP if the TCP transport fails.
 - Step 8** In the Format field, indicate whether EMBLEM-format logging is to be used as follows:
 - N/A—Indicates that you do not want to enable EMBLEM-format logging.
 - Emblem—Indicates that EMBLEM-format logging is to be enabled for each syslog server. If you use Cisco Resource Manager Essentials (RME) software to collect and process syslog messages on your network, enable EMBLEM-format logging so that RME can handle them. Similarly, UDP needs to be enabled because the Cisco Resource Manager Essentials (RME) syslog analyzer supports only UDP syslog messages.
 - Step 9** Do one of the following:
 - Click **Deploy Now** to deploy this configuration on the ACE appliance.
 - Click **Cancel** to exit the procedure without saving your entries and to return to the Log Host table.
 - Click **Add Another** to configure another syslog host.
-

Related Topics

- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring Syslog Log Messages, page 4-17](#)
- [Configuring Syslog Log Rate Limits, page 4-18](#)

Configuring Syslog Log Messages

After configuring basic syslog characteristics (see the “[Configuring Virtual Context Syslog Logging](#)” [section on page 4-12](#)), you can configure the log host, log messages, and log rate limits. The tabs for these attributes appear beneath the Syslog configuration screen.

Use this procedure to configure Syslog log messages.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Choose Config > Virtual Contexts > context > System > Syslog .
The Syslog configuration screen appears. |
| Step 2 | Click the Log Message tab.
The Log Message table appears. |
| Step 3 | Click Add to add a new entry to this table, or select an existing entry, and then click Edit to modify it.
The Log Message configuration screen appears. |
| Step 4 | In the Message Id field, select the system log message ID of the syslog messages that are to be sent to the syslog server or that are not to be sent to the syslog server. |
| Step 5 | Check the Enable State check box to indicate that logging is enabled for the specified message ID.
Clear the check box to indicate that logging is not enabled for the specified message ID. If you check the Enable State check box, the Log Level field appears. |
| Step 6 | In the Log Level field, select the desired level of syslog messages to be sent to the syslog server, using the levels identified in Table 4-4 . |
| Step 7 | Do one of the following: <ul style="list-style-type: none">• Click Deploy Now to deploy this configuration on the ACE appliance.• Click Cancel to exit the procedure without saving your entries and to return to the Log Message table.• Click Add Another to save your entries and to configure additional syslog message entries for this virtual context. |
-

Related Topics

- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring Syslog Log Hosts, page 4-16](#)
- [Configuring Syslog Log Rate Limits, page 4-18](#)

Configuring Syslog Log Rate Limits

After configuring basic syslog characteristics (see the [“Configuring Virtual Context Syslog Logging” section on page 4-12](#)), you can configure the log host, log messages, and log rate limits. The tabs for these attributes appear beneath the Syslog configuration screen.

Use this procedure to limit the rate at which the ACE appliance generates messages in the syslog.

Procedure

-
- Step 1** Choose **Config > Virtual Contexts > context > System > Syslog**.
The Syslog configuration screen appears.
- Step 2** Click the **Log Rate Limit** tab.
The Log Rate Limit table appears.
- Step 3** Click **Add** to add a new entry to this table, or select an existing entry, and then click **Edit** to modify it.
The Log Rate Limit configuration screen appears.
- Step 4** In the Type field, indicate the method by which syslog messages are to be limited as follows:
- Choose **Level** to limit syslog messages by syslog level. In the Level field, select the level of syslog messages to be sent to the syslog server, using the levels identified in [Table 4-4](#).
 - Choose **Message** to limit syslog messages by message identification number. In the Message Id field, select the syslog message ID for those messages for which you want to suppress reporting.
- Step 5** Check the **Unlimited** check box to indicate that limits are not to be applied to system message logging.
Clear the **Unlimited** check box to indicate that limits are to be applied to system message logging. If you clear the Unlimited check box, the Rate and Time Interval fields appear.
- Step 6** If you clear the Unlimited check box, specify the limits to apply to system message logging as follows:
- a. In the Rate field, enter the number at which syslog message creation is to be limited. When this limit is reached, the ACE appliance limits the creation of new syslog messages to be no greater than the specified rate. Valid entries are integers from 0 to 2147483647.
 - b. In the Time Interval (Seconds) field, enter the length of time (in seconds) over which the system message logs should be limited. The default time interval is one second. For example, if you enter 42 in the Rate field and 60 in the Time Interval (Seconds) field, the ACE appliance limits the creation of syslog messages that are sent to a maximum of 42 messages in that 60-second period. Valid entries are from 0 to 2147483647 seconds.
- Step 7** Do one of the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
 - Click **Cancel** to exit the procedure without saving your entries and to return to the Log Rate Limit table.
 - Click **Add Another** to save your entries and to add another entry to the Log Rate Limit table.
-

Related Topics

- [Configuring Virtual Contexts, page 4-7](#)
- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring Syslog Log Hosts, page 4-16](#)

- [Configuring Syslog Log Messages, page 4-17](#)

Configuring SNMP for Virtual Contexts

This section describes how to configure the SNMP attributes for a virtual context and contains the following topics:

- [Configuring Basic SNMP Attributes, page 4-19](#)
- [Configuring SNMP Version 2c Communities, page 4-20](#)
- [Configuring SNMP Version 3 Users, page 4-21](#)
- [Configuring SNMP Trap Destination Hosts, page 4-23](#)
- [Configuring SNMP Notifications, page 4-25](#)

Configuring Basic SNMP Attributes

Use this procedure to configure basic SNMP attributes for use with this virtual context.

Procedure

- Step 1** Choose **Config > Virtual Contexts > context > System > SNMP**.
The SNMP configuration screen appears.
- Step 2** Enter SNMP attributes (see [Table 4-6](#)).

Table 4-6 *SNMP Attributes*

Field	Description
Contact Information	Enter contact information for the SNMP server within the virtual context as a text string with a maximum of 240 characters including spaces. In addition to a name, you might want to include a phone number or e-mail address. To include spaces, add quotation marks at the beginning and end of the entry.
Location	Enter the physical location of the system as a text string with a maximum of 240 characters including spaces. To include spaces, add quotation marks at the beginning and end of the entry.
Unmask Community	Check the check box to unmask the snmpCommunityName and snmpCommunitySecurityName OIDs of the SNMP-COMMUNITY-MIB. Clear the check box to mask these OIDs. By default, they are masked (the check box is unchecked).

Table 4-6 SNMP Attributes (continued)

Field	Description
Trap Source Interface	Enter a valid VLAN number that identifies the interface from which the SNMP traps originate.
IETF Trap	<p>Check the check box to indicate that the ACE appliance is to send linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings, consisting of ifIndex, ifAdminStatus, and ifOperStatus.</p> <p>Clear the check box to indicate that the ACE appliance is not to send linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings. Instead, the ACE appliance sends Cisco var-binds by default.</p>

Step 3 Click **Deploy Now** to deploy this configuration on the ACE appliance.

To configure other SNMP attributes, see the following topics:

- [Configuring SNMP Version 2c Communities, page 4-20](#)
- [Configuring SNMP Version 3 Users, page 4-21](#)
- [Configuring SNMP Trap Destination Hosts, page 4-23](#)
- [Configuring SNMP Notifications, page 4-25](#)

Related Topic

- [Configuring Virtual Contexts, page 4-7](#)

Configuring SNMP Version 2c Communities

After configuring basic SNMP information for a virtual context (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.



Note All SNMP communities in ACE Appliance Device Manager are read-only communities and all communities belong to the group *network monitors*.

Use this procedure to configure SNMP version 2c communities for a virtual context.

Assumption

You have configured at least one SNMP contact (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19).

Procedure

Step 1 Choose **Config > Virtual Contexts > context > System > SNMP**.

The SNMP configuration screen appears.

Step 2 Click the **SNMP v2c Configuration** tab.

The SNMP v2c Configuration table appears.

Step 3 Click **Add** to add an SNMP v2c community.

The SNMP v2c Configuration screen appears.



Note You cannot modify an existing SNMP v2c community. Instead, delete the existing SNMP v2c community, and then add a new one.

Step 4 In the Read-Only Community field, enter the SNMP v2c community name for this context.

Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entry and to return to the SNMP v2c Community table.
- Click **Add Another** to save your entry and to configure another SNMP community for this virtual context. The screen refreshes and you can enter another community name.

Related Topics

- [Configuring Virtual Contexts, page 4-7](#)
- [Configuring SNMP Version 3 Users, page 4-21](#)
- [Configuring SNMP Trap Destination Hosts, page 4-23](#)
- [Configuring SNMP Notifications, page 4-25](#)

Configuring SNMP Version 3 Users

After configuring basic SNMP information for a virtual context (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.

Use this procedure to configure SNMP version 3 users for a virtual context.

Assumption

You have configured at least one SNMP contact (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19).

Procedure

Step 1 Choose **Config > Virtual Contexts > context > System > SNMP**.

The SNMP configuration screen appears.

Step 2 Click the **SNMP v3 Configuration** tab.

The SNMP v3 Configuration table appears.

Step 3 Click **Add** to add users, or select an existing entry, and then **Edit** to modify it.

The SNMP v3 Configuration screen appears.

Step 4 Enter SNMP v3 user attributes (see [Table 4-7](#)).

Table 4-7 *SNMP v3 User Configuration Attributes*

Field	Description
User Name	Enter the SNMP v3 username. Valid entries are unquoted text strings with no spaces and a maximum of 24 characters.
Authentication Algorithm	Select the authentication algorithm to be used for this user. <ul style="list-style-type: none"> N/A—Indicates that no authentication is to be used. Message Digest (MD5)—Indicates that Message Digest 5 is to be used as the authentication mechanism. Secure Hash Algorithm (SHA)—Indicates that Secure Hash Algorithm is to be used as the authentication mechanism.
Authentication Password	Appears if you select an authentication algorithm. The ACE appliance automatically updates the password for the CLI user with the SNMP authentication password. Enter the authentication password for this user as follows: <ul style="list-style-type: none"> If the passphrases are specified in clear text, enter an unquoted text string with no space that is from 8 to 64 alphanumeric characters in length. The password length can be an odd or even value. If use of a localized key is enabled, enter an unquoted text string with no space that is from 8 to 130 alphanumeric characters in length. The password length must be an even value.
Confirm	Appears if you select an authentication algorithm. Reenter the authentication password.
Localized	Appears if you select an authentication algorithm. This field will be always selected to True . <ul style="list-style-type: none"> True—Indicates that the password is in localized key format for encryption.
Privacy	Appears if you select an authentication algorithm. Indicate whether encryption attributes are to be configured for this user: <ul style="list-style-type: none"> N/A—Indicates that no encryption attributes are specified. False—Indicates that encryption parameters are not to be configured for this user. True—Indicates that encryption parameters are to be configured for this user.

Table 4-7 *SNMP v3 User Configuration Attributes (continued)*

Field	Description
AES 128	<p>Appears if you set Privacy to True.</p> <p>Indicate whether the 128-byte Advanced Encryption standard (AES) algorithm is to be used for privacy. AES is a symmetric cipher algorithm and is one of the privacy protocols for SNMP message encryption.</p> <ul style="list-style-type: none"> N/A—Indicates that no standard is specified. False—Indicates that AES 128 is not be used for privacy. True—Indicates that AES 128 is to be used for privacy.
Privacy Password	<p>Appears if you set Privacy to True. Enter the user encryption password as follows:</p> <ul style="list-style-type: none"> If the passphrases are specified in clear text, enter an unquoted text string with no space that is from 8 to 64 alphanumeric characters in length. The password length can be an odd or even value. If use of a localized key is enabled, enter an unquoted text string with no space that is from 8 to 130 alphanumeric characters in length. The password length must be an even value.
Confirm	<p>Appears if you set Privacy to True.</p> <p>Reenter the privacy password.</p>

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the SNMP v3 Configuration table.
- Click **Add Another** to save your entries and to add another entry to the SNMP v3 Configuration table. The screen refreshes and you can enter another SNMP v3 user.

Related Topics

- [Configuring Virtual Contexts, page 4-7](#)
- [Configuring SNMP Version 2c Communities, page 4-20](#)
- [Configuring SNMP Trap Destination Hosts, page 4-23](#)
- [Configuring SNMP Notifications, page 4-25](#)

Configuring SNMP Trap Destination Hosts

To receive SNMP notifications you must configure:

- At least one SNMP trap destination host. This section describes how to do this.
- At least one type of notification. See the [“Configuring SNMP Notifications” section on page 4-25](#).

After configuring basic SNMP information for a virtual context (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.

Use this procedure to configure SNMP trap destination hosts for a virtual context.

Assumption

You have configured at least one SNMP contact (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19).

Procedure

-
- Step 1** Choose **Config > Virtual Contexts > context > System > SNMP**.
The SNMP configuration screen appears.
- Step 2** Click the **Trap Destination Host** tab.
The Trap Destination Host table appears.
- Step 3** Click **Add** to add a host, or select an existing entry in the table, and then **Edit** to modify it.
The Trap Destination Host configuration screen appears.
- Step 4** Configure the SNMP trap destination host using the information in [Table 4-8](#).

Table 4-8 *SNMP Trap Destination Host Configuration Attributes*

Field	Description
IP Address	Enter the IPv4 address of the server that is to receive SNMP notifications.
Port	Enter the port to be used for SNMP notification. The default port is 162.
Version	Select the version of SNMP used to send traps: <ul style="list-style-type: none"> V1—Indicates that SNMP version 1 is to be used to send traps. This option is not available for use with SNMP inform requests. V2c—Indicates that SNMP version 2c is to be used to send traps. V3—Indicates that SNMP version 3 is to be used to send traps. This version is the most secure model because it allows packet encryption.
Community	Enter the SNMP community string or username to be sent with the notification operation. Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.
Security Level	This field appears if V3 is the selected version. Select the level of security that is to be implemented: <ul style="list-style-type: none"> Auth—Indicates that Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) are to be used for packet authentication. Noauth—Indicates that the noAuthNoPriv security level is to be used. Priv—Indicates that Data Encryption Standard (DES) is to be used for packet encryption.

- Step 5** Do one of the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Trap Destination Host table.
- Click **Add Another** to save your entries and to add another entry to the Trap Destination Host table. The screen refreshes and you can add another trap destination host.

Related Topics

- [Configuring Virtual Contexts, page 4-7](#)
- [Configuring SNMP Version 2c Communities, page 4-20](#)
- [Configuring SNMP Version 3 Users, page 4-21](#)
- [Configuring SNMP Notifications, page 4-25](#)

Configuring SNMP Notifications

After configuring basic SNMP information for a virtual context (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.

To receive SNMP notifications you must configure:

- At least one SNMP trap destination host. See the “[Configuring SNMP Trap Destination Hosts](#)” section on page 4-23.
- At least one type of notification as described in this section.

Use this procedure to configure SNMP notification for a virtual context.

Prerequisites

- At least one SNMP contact has been configured (see the “[Configuring SNMP for Virtual Contexts](#)” section on page 4-19).
- At least one SNMP server host has been configured (see the “[Configuring SNMP Trap Destination Hosts](#)” section on page 4-23).

Procedure

Step 1 Choose **Config > Virtual Contexts > context > System > SNMP**.

The SNMP configuration screen appears.

Step 2 Click the **SNMP Notification** tab.

The SNMP Notification table appears.

Step 3 Click **Add** to add a new entry.

The SNMP Notification configuration screen appears.



Note You cannot modify an existing entry. Instead, delete the existing notification entry and then add a new one.

Step 4 In the Options field, choose the type of notifications to be sent to the SNMP host.

For the notification types, see [Table 4-9](#).

Table 4-9 *Types of Notification*

Notification Type	Description	Context
Bandwidth	Notifications are sent that indicate changes to the bandwidth usage (see the “Setting Resource Usage Thresholds to Receive SNMP Notifications” section on page 4-42).	All
Concurrent Connections	Notifications are sent that indicate changes to the concurrent connections (see the “Setting Resource Usage Thresholds to Receive SNMP Notifications” section on page 4-42)	All
Connection Rate	Notifications are sent that indicate changes to the connection rates (see the “Setting Resource Usage Thresholds to Receive SNMP Notifications” section on page 4-42).	All
License	SNMP license notifications are to be sent.	Admin
Rate Limit	Notifications are sent when the threshold settings for the attributes associated with the rate limit are breached. For more information, see the “Setting Resource Usage Thresholds to Receive SNMP Notifications” section on page 4-42.	All
Real Server	Notifications are sent when the threshold settings for the attributes associated with the real server are breached.	All
Real Server Bandwidth	Notifications are sent that indicate changes to the aggregated bandwidth usage at the real server level. For more information, see the “Setting Resource Usage Thresholds to Receive SNMP Notifications” section on page 4-42).	All
Real Server Concurrent Connections	Notifications are sent that indicate changes to the concurrent connections at the real server level.	All
Real Server Connection Rate	Notifications are sent that indicate changes to the connection rates at the real server level.	All
SLB	Server load-balancing notifications are to be sent.	All
SLB Real Server	Notifications of real server state changes are to be sent.	All
SLB Server Farm	Notifications of server farm state changes are to be sent.	All
SLB Virtual Server	Notifications of virtual server state changes are to be sent.	All
SNMP	SNMP notifications are to be sent.	All
SNMP Authentication	Notifications of incorrect community strings in SNMP requests are to be sent.	All
SNMP Cold-Start	SNMP agent restart notifications are to be sent after a cold restart (full power cycle) of the ACE.	Admin
SNMP Link-Down	Notifications are to be sent when a VLAN interface is down.	All
SNMP Link-Up	Notifications are to be sent when a VLAN interface is up.	All
Syslog	Error message notifications (Cisco Syslog MIB) are to be sent.	All
System	Notifications are sent when the threshold settings for the attributes associated with the system level are breached.	Admin

Table 4-9 Types of Notification (continued)

Notification Type	Description	Context
System Active SSL Connections	Notifications are sent that indicate changes to the aggregated active SSL connections. For more information, see the “Setting Resource Usage Thresholds to Receive SNMP Notifications” section on page 4-42). Note This resource option is not available with the ACE NPE software version (see the “Information About the ACE No Payload Encryption Software Version” section on page 1-2).	Admin
System Bandwidth	Notifications are sent that indicate changes to the aggregated bandwidth usage. For more information, see the “Setting Resource Usage Thresholds to Receive SNMP Notifications” section on page 4-42).	Admin
System Concurrent Connections	Notifications are sent that indicate changes to the concurrent connections.	Admin
System Connection Rate	Notifications are sent that indicate changes to the connection rates at the system level.	Admin
System CPU Utilization	Notifications are sent that indicate changes to the CPU utilization at the system level.	Admin
System Memory Utilization	Notifications are sent that indicate changes to the memory utilization at the system level.	Admin
VIP	Notifications are sent when the threshold settings for the attributes associated with VIP are breached.	All
VIP Bandwidth	Notifications are sent that indicate changes to the bandwidth usage at the VIP level.	All
VIP Concurrent Connections	Notifications are sent that indicate changes to the concurrent connections at the VIP level.	All
VIP Connection Rate	Notifications are sent that indicate changes to the connection rate at the VIP level.	All
Virtual Context	Virtual context notifications are to be sent.	Admin

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your selection and to return to the SNMP Notification table.
- Click **Add Another** to save your entries and to add another entry to the SNMP Notification table. The screen refreshes and you can select another SNMP notification option.

Related Topics

- [Configuring Virtual Contexts, page 4-7](#)
- [Configuring SNMP Version 2c Communities, page 4-20](#)
- [Configuring SNMP Version 3 Users, page 4-21](#)
- [Setting Resource Usage Thresholds to Receive SNMP Notifications, page 4-42](#)

Configuring Virtual Context Global Traffic Policies

With the ACE Appliance Device Manager, you can apply traffic policies to a specific VLAN interface or to all VLAN interfaces in the same virtual context.

Use this procedure to apply a policy to all VLAN interfaces in the selected context.

To apply a policy to a specific VLAN, see the [“Configuring Traffic Policies” section on page 12-1](#).



Note You cannot modify an existing policy. Instead, delete the existing global policy, and then create a new one.

Assumption

A Layer 3/Layer 4 or Management policy map has been configured for this virtual context. For more information, see the [“Configuring Virtual Context Policy Maps” section on page 12-34](#).

Procedure

Step 1 Choose **Config > Virtual Contexts > context > System > Global Policies**.

The Global Policies table appears.

Step 2 Click **Add** to add a new global policy.

The Global Policies configuration screen appears.



Note You cannot modify an existing policy. Instead, delete the existing global policy, and then create a new one.

Step 3 In the Policy Maps field, choose the policy map that you want to apply to all VLANs in this context.

Click the **Add** button to create or edit the policy map.

Step 4 In the Direction field, verify that the policy is being applied to incoming communications.

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Global Policies table.
- Click **Add Another** to save your entries and to configure another global policy for this context.

Related Topics

- [Using Virtual Contexts, page 4-2](#)
- [Configuring Virtual Context Primary Attributes, page 4-11](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring Traffic Policies, page 12-1](#)

Managing ACE Appliance Licenses

**Note**

This functionality is available for only Admin contexts.

Cisco offers licenses for ACE appliances that let you increase performance throughput, the number of default contexts, SSL TPS (transactions per second), and HTTP compression performance. For more information on these licenses, refer to the *Administration Guide, Cisco ACE Application Control Engine* on cisco.com.

You can view, install, remove, or update ACE appliance licenses using the ACE Appliance Device Manager.

Installing or updating an ACE appliance license involves two processes:

- Copying the license from a remote network server to the disk0: file system in Flash memory on the ACE appliance.
- Installing or updating the license on the ACE appliance.

You can use the ACE appliance Device Manager to perform both processes from a single dialog box. If you previously copied the license to disk0: on the ACE by using the **copy** CLI command, you can use this dialog box to install the new license or upgrade license on your ACE.

Related Topics

- [Viewing ACE Appliance Licenses, page 4-29](#)
- [Installing ACE Appliance Licenses, page 4-30](#)
- [Updating ACE Appliance Licenses, page 4-32](#)
- [Uninstalling ACE Appliance Licenses, page 4-33](#)
- [Displaying the File Contents of a License, page 4-34](#)

Viewing ACE Appliance Licenses

**Note**

This functionality is available for only Admin contexts.

Use this procedure to view the licenses that are currently installed on an ACE appliance.

Procedure

-
- Step 1** Choose **Config > Virtual Contexts**.
- The All Virtual Context table appears.
- Step 2** Choose the Admin context whose ACE appliance licenses you want to view, and then click **System > Licenses**.
- The following license tables appear:
- License Status Table—Provides a summary of the license status for the ACE, including:
 - Compression performance in megabits or Gigabits per second
 - Application acceleration and optimization in the number of concurrent connections

- SSL transactions per second



Note The SSL transactions per second license does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

- Number of supported virtual contexts
- ACE appliance bandwidth in Gigabits per second
- Installed License Files Table—Lists all installed licenses with their filenames, vendors, and expiration (expiry) dates.

Related Topics

- [Managing ACE Appliance Licenses, page 4-29](#)
- [Installing ACE Appliance Licenses, page 4-30](#)
- [Updating ACE Appliance Licenses, page 4-32](#)
- [Uninstalling ACE Appliance Licenses, page 4-33](#)
- [Displaying the File Contents of a License, page 4-34](#)

Installing ACE Appliance Licenses



Note This functionality is available for only Admin contexts.

Use this procedure to copy and install a new or upgrade ACE appliance license from a remote server onto the ACE appliance.

Assumption

- You have received the proper software license key for the ACE appliance.
- ACE appliance licenses are available on a remote server for importing to the ACE appliance, or you have received the software license key and have copied the license file to the disk0: filesystem on the ACE appliance using the **copy disk0:** CLI command.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

- Step 1** Choose **Config > Virtual Contexts**.
The All Virtual Contexts table appears.
- Step 2** Choose the Admin context you want to import and install a license for, and then click **System > Licenses**.
The License Status Table and Installed License Files Table appear listing all installed licenses.
- Step 3** Click **Install**.

The Install an ACE License dialog box appears.

- Step 4** (Optional) If the license currently exists on the ACE disk0: file system in Flash memory, do the following:
- In the Select an Option to Locate a License File section of the dialog box, click the **Select a license file on the ACE** option.
 - In the Select a License File on the Device (disk0) section of the dialog box, from the drop-down list, choose the name of the license file.
 - Go to Step 10.
- Step 5** (Optional) If the license must be copied to the disk0: file system in Flash memory, in the Select an Option to Locate a License File section of the dialog box, click the **Import a license file from remote system** option. Go to Step 6.
- Step 6** In the Protocol To Connect To Remote System field, choose the protocol to be used to import the license file from the remote server to the ACE as follows:
- If you choose FTP, the User Name and Password fields appear. Go to Step 7.
 - If you choose SFTP, the User Name and Password fields appear. Go to Step 7.
 - If you choose TFTP, go to Step 8.
- Step 7** (Optional) If you chose FTP or SFTP, do the following:
- In the User Name field, enter the username of the account on the network server.
 - In the Password field, enter the password for the user account.
- Step 8** In the Remote System IP Address field, enter the host IPv4 address of the remote server. For example, your entry might be 192.168.11.2.
- Step 9** In the License Path In Remote System field, enter the host path and filename of the license file on the remote server in the format */path/filename* where:
- path* represents the directory path of the license file on the remote server.
 - filename* represents the filename of the license file on the remote server.
- For example, your entry might resemble */usr/bin/ACE-VIRT-020.lic*.
- Step 10** Do one of the following:
- Click **Install** to accept your entries and to install the license file.
 - Click **Cancel** to exit this procedure without installing the license file and to return to the Licenses table.
- Step 11** (Optional) After installing an ACE license, we recommend that you manually synchronize the ACE Admin context with the CLI to ensure that DM accurately displays the monitored resource usage information (Monitor > Virtual Contexts > Resource Usage).
- For information about synchronizing the Admin context, see the [“Synchronizing Virtual Context Configurations” section on page 4-79](#).
-

Related Topics

- [Managing ACE Appliance Licenses, page 4-29](#)
- [Viewing ACE Appliance Licenses, page 4-29](#)
- [Updating ACE Appliance Licenses, page 4-32](#)

- [Uninstalling ACE Appliance Licenses, page 4-33](#)
- [Displaying the File Contents of a License, page 4-34](#)

Updating ACE Appliance Licenses



Note

This functionality is available for only Admin contexts.

ACE Appliance Device Manager allows you to convert demonstration licenses to permanent licenses and to upgrade permanent licenses to increase the number of virtual contexts.

Use this procedure to install ACE appliance update licenses.

Assumption

- You have received the proper update software license for the ACE appliance.
- ACE appliance licenses are available on a remote server for importing to the ACE appliance, or you have received the update software license and have copied the license file to the disk0: filesystem on the ACE appliance using the **copy disk0:** CLI command.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

-
- Step 1** Choose **Config > Virtual Contexts**.
- The All Virtual Contexts table appears.
- Step 2** Choose the Admin context with the license you want to update, and then click **System > Licenses**.
- The License Status Table and Installed License Files Table appear listing all installed licenses.
- Step 3** Select the license to be updated, and then click **Update**.
- The Update License On The ACE dialog box appears.
- Step 4** (Optional) If the update license currently exists on the ACE disk0: file system in Flash memory, do the following:
- a. In the Select an Option to Locate a License File section of the dialog box, click the **Select a license file on the ACE** option.
 - b. In the Select a License File on the Device (disk0) section of the dialog box, choose the name of the update license file from the drop-down list.
 - c. Go to Step 10.
- Step 5** (Optional) If the update license must be copied to the disk0: file system in Flash memory, in the Select an Option to Locate a License File section of the dialog box, click the **Import a license file from remote system** option and go to Step 6.
- Step 6** In the Protocol To Connect To Remote System field, choose the protocol to be used to import the update license file from the remote server to the ACE as follows:
- If you choose FTP, the User Name and Password fields appear. Go to Step 7.
 - If you choose SFTP, the User Name and Password fields appear. Go to Step 7.
 - If you choose TFTP, go to Step 8.

- Step 7** (Optional) If you chose FTP or SFTP, do the following:
- In the User Name field, enter the username of the account on the network server.
 - In the Password field, enter the password for the user account.
- Step 8** In the Remote System IP Address field, enter the host IPv4 address of the remote server.
For example, your entry might be 192.168.11.2.
- Step 9** In the Licence Path In Remote System field, enter the host path and filename of the license file on the remote server in the format */path/filename* where:
- path* represents the directory path of the license file on the remote server.
 - filename* represents the filename of the license file on the remote server.
- For example, your entry might be /usr/bin/ACE-VIRT-020.lic.
- Step 10** Do one of the following:
- Click **Update** to update the license and to return to the License table. The License table displays the updated information.
 - Click **Cancel** to exit this procedure without updating the license and to return to the License table.
- Step 11** (Optional) After updating an ACE license, we recommend that you manually synchronize the ACE Admin context with the CLI to ensure that DM accurately displays the monitored resource usage information (Monitor > Virtual Contexts > ACE > Resource Usage).
For information about synchronizing the Admin context, see the [“Synchronizing Virtual Context Configurations” section on page 4-79](#).

Related Topics

- [Managing ACE Appliance Licenses, page 4-29](#)
- [Viewing ACE Appliance Licenses, page 4-29](#)
- [Installing ACE Appliance Licenses, page 4-30](#)
- [Uninstalling ACE Appliance Licenses, page 4-33](#)
- [Displaying the File Contents of a License, page 4-34](#)

Uninstalling ACE Appliance Licenses



Note

This functionality is available for only Admin contexts.



Caution

Removing licenses can affect an ACE appliance's bandwidth or performance. For detailed information on the effect of license removal on your ACE appliance, see the *Administration Guide, Cisco ACE Application Control Engine*.

Use this procedure to remove ACE appliance licenses.

Assumption

This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Choose the Admin context with the license you want to remove, and then click **System > Licenses**.

Step 3 In the Installed License Files table, choose the license to be removed.

Step 4 Click **Uninstall**.

A dialog box appears, asking you to confirm the license removal process.



Note Removing licenses can affect the number of contexts, ACE appliance bandwidth, or SSL TPS (transactions per second). Be sure you understand the effect of removing the license on your environment before continuing.

Step 5 Click **OK** to confirm the removal or **Cancel** to stop the removal process.

If you click OK, a status window appears with the status of license removal. When the license has been removed, the Licenses table refreshes without the deleted license.

Step 6 (Optional) After uninstalling an ACE license, we recommend that you manually synchronize the ACE Admin context with the CLI to ensure that DM accurately displays the monitored resource usage information (Monitor > Virtual Contexts > Resource Usage).

For information about synchronizing the Admin context, see the [“Synchronizing Virtual Context Configurations” section on page 4-79](#).

Related Topics

- [Managing ACE Appliance Licenses, page 4-29](#)
- [Installing ACE Appliance Licenses, page 4-30](#)
- [Updating ACE Appliance Licenses, page 4-32](#)
- [Viewing ACE Appliance Licenses, page 4-29](#)
- [Displaying the File Contents of a License, page 4-34](#)

Displaying the File Contents of a License



Note This functionality is available for only Admin contexts.

Use this procedure to display file content information about ACE licenses.

Procedure

-
- Step 1** Choose **Config > Virtual Contexts**.
The All Virtual Contexts table appears.
- Step 2** Choose the Admin context with the license information you want to view, and then choose **System > Licenses**.
The License Status Table and Installed License Files Table appear listing all installed licenses.
- Step 3** Choose the installed license file with the information that you want to display, and click **View**.
DM displays the output of the **show license file C LI** command.
For example:
- ```
ACE-AP-C-500-LIC.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ACE-AP-C-500-LIC cisco 1.0 permanent 1 \
NOTICE="<LicFileID>lic.conf</LicFileID><LicLineID>0</LicLineID> \
<PAK>dummyPak</PAK>" SIGN=222C4BCAD092
```
- Step 4** Click **Close** when you finish viewing the license file information.
- 

### Related Topics

- [Installing ACE Appliance Licenses, page 4-30](#)
- [Updating ACE Appliance Licenses, page 4-32](#)

## Managing Resource Classes

Resource classes are the means by which you manage virtual context access to ACE appliance resources, such as concurrent connections or bandwidth rate. ACE appliances are preconfigured with a default resource class that is applied to the Admin context and any user context upon creation. The default resource class is configured to allow a context to operate within a range that can vary from no resource access (0%) to complete resource access (100%). When you use the default resource class with multiple contexts, you run the risk of oversubscribing ACE appliance resources. This means that the ACE appliance permits all contexts to have full access to all resources on a first-come, first-served basis. When a resource is utilized to its maximum limit, the ACE appliance denies additional requests made by any context for that resource.

To avoid oversubscribing resources and to help guarantee access to a resource by any context, you can create customized resource classes that you associate with one or more contexts. A context becomes a member of the resource class when you make the association. Creating a resource class allows you to set limits on the minimum and maximum amounts of each ACE appliance resource that a member context is entitled to use. You define the minimum and maximum values as a percentage of the whole. For example, you can create a resource class that allows its member contexts access to no less than 25% of the total number of SSL connections that the ACE appliance supports.

You can limit and manage the allocation of the following ACE appliance resources:

- ACL memory
- Application acceleration connections
- Buffers for syslog messages and TCP out-of-order (OOO) segments

- Concurrent connections (through-the-ACE traffic)
- Management connections (to-the-ACE traffic)
- HTTP compression percentage
- Proxy connections
- Set resource limit as a rate (number per second)
- Regular expression (regex) memory
- SSL connections



**Note** Managing the SSL connections resource does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

- Sticky entries
- Static or dynamic network address translations (Xlates)

[Table 4-10](#) identifies and defines the resources that you can establish for resource classes.

## Resource Allocation Constraints



**Note**

This functionality is available for only Admin contexts.

The following resources are critical for maintaining connectivity to the Admin context:

- Rate Bandwidth
- Rate Management Traffic
- Rate SSL Connections
- Rate Connections
- Management Connections
- Concurrent Connections



**Caution**

If you allocate 100% of these resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost.

We recommend that you create a resource class specifically for the Admin context and apply it to the context so that you can maintain IP connectivity.

Table 4-10 Resource Class Attributes

| Resource                 | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All                      | Limits all resources to the specified value for all contexts assigned to this resource class, except for management traffic bandwidth. Management traffic bandwidth remains at the default values until you explicitly configure a minimum value for management traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Acceleration Connections | Percentage of application acceleration connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ACL Memory               | Percentage of memory allocated for ACLs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Buffer Syslog            | Percentage of the syslog buffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Concurrent Connections   | Percentage of simultaneous connections.<br><b>Note</b> If you consume all Concurrent Connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| HTTP Compression         | Percentage of compression for HTTP data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Management Connections   | Percentage of management connections.<br><b>Note</b> If you consume all Management Connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Proxy Connections        | Percentage of proxy connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Rate Bandwidth           | <p>Percentage of context throughput. This attribute limits the total ACE throughput in bytes per second for one or more contexts.</p> <p><b>Note</b> If you consume all rate bandwidth by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.</p> <p>The maximum bandwidth rate per context is determined by your bandwidth license. By default, the ACE supports 1 Gigabit per second (Gbps) appliance throughput. You can upgrade the ACE with an optional 2-Gbps bandwidth license. When you configure a minimum bandwidth value for a resource class in the ACE, the ACE subtracts that configured value from the total bandwidth maximum value of all contexts in the ACE, regardless of the resource class with which they are associated. The total bandwidth rate of a context consists of the following two components:</p> <ul style="list-style-type: none"> <li>Throughput—Limits through-the-ACE traffic. This is a derived value (you cannot configure it directly) and it is equal to the bandwidth rate minus the mgmt-traffic rate for the 1-Gbps and 2-Gbps licenses.</li> <li>Management Traffic—Limits management (to-the-ACE) traffic in bytes per second. To guarantee a minimum amount of management traffic bandwidth, you must explicitly allocate a minimum percentage to management traffic using the Resource Classes table (<b>Config &gt; Virtual Contexts &gt; admin context &gt; System &gt; Resource Class</b>). When you allocate a minimum percentage of bandwidth to management traffic, the ACE subtracts that value from the maximum available management traffic bandwidth for all contexts in the ACE.</li> </ul> |
| Rate Connections         | Percentage of connections of any kind.<br><b>Note</b> If you consume all Rate Connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 4-10 Resource Class Attributes (continued)

| Resource                | Definition                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rate Inspect Connection | Percentage of application protocol inspection connections for FTP and RTSP.                                                                                                                                                                                                                                                                                                                 |
| Rate MAC Miss           | Percentage of messages destined for the ACE appliance that are sent to the control plane when the encapsulation is not correct in packets.                                                                                                                                                                                                                                                  |
| Rate Management Traffic | Percentage of management traffic connections.<br><b>Note</b> If you consume all Rate Management Traffic by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.                                                                                                                                                                                           |
| Rate SSL Connections    | <b>Note</b> This resource option is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).<br>Percentage of SSL connections.<br><b>Note</b> If you consume all Rate Management Traffic by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost. |
| Rate Syslog             | Percentage of syslog messages per second.                                                                                                                                                                                                                                                                                                                                                   |
| Regular Expressions     | Percentage of regular expression memory.                                                                                                                                                                                                                                                                                                                                                    |
| Sticky                  | Percentage of entries in the sticky table.                                                                                                                                                                                                                                                                                                                                                  |
| Xlates                  | Percentage of network and port address translations entries.                                                                                                                                                                                                                                                                                                                                |

**Related Topics**

- [Adding Resource Classes, page 4-38](#)
- [Modifying Resource Classes, page 4-40](#)
- [Deleting Resource Classes, page 4-41](#)
- [Viewing Resource Class Use on Virtual Contexts, page 4-41](#)

## Adding Resource Classes

**Note**

This functionality is available for only Admin contexts.

Resource classes are used when provisioning services, establishing virtual contexts, managing devices, and monitoring virtual context resource consumption.

Defining a resource class does not automatically apply it to a context. New resource classes are applied only when a resource class is assigned to a virtual context.

**Caution**

If you allocate 100% of the resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost. For more information, see the [“Resource Allocation Constraints”](#) section on page 4-36.

Use this procedure to create a new resource class.



### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > admin context > System > Resource Class**.  
The Resource Classes table appears.
- Step 2** Click **Add** to create a new resource class.  
The New Resource Class configuration screen appears.
- Step 3** In the Name field, enter a unique name for this resource class.  
Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
- Step 4** To use the same values for each resource, enter the following information in the All row (See [Table 4-10](#) for a description of the resources):
- In the Min. field, enter the minimum percentage of each resource you want to allocate to this resource class. Valid entries are numbers from 0 to 100 including those with decimals in increments of .01.
  - In the Max. field, choose the maximum percentage of each resource you want to allocate to this resource class:
    - Equal To Min.—Indicates that the maximum percentage allocated for each resource is equal to the minimum specified in the Min. field.
    - Unlimited—Indicates that there is no upper limit on the percentage of each resource that can be allocated for this resource class.
- Step 5** To use different values for the resources, for each resource, choose the method for allocating resources:
- Select **Default** to use the values specified in [Step 4](#).
  - Choose **Min.** to enter a specific minimum value for the resource. In the Min. field, enter the minimum percentage of this resource you want to allocate to this resource class. For example, for ACL memory, you would enter 10 in the Min. field to indicate that you want to allocate a minimum of 10 percent of the available ACL memory to this resource class.
- Step 6** If you chose **Min.**, in the Max. field, choose the maximum percentage of the resource you want to allocate to this resource class:
- Equal To Min.**—Indicates that the maximum percentage allocated for this resource is equal to the minimum specified in the Min. field.
  - Unlimited**—Indicates that there is no upper limit on the percentage of the resource that can be allocated for this resource class.
- Step 7** When you finish allocating the resources for this resource class, do one of the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance. The ACE Appliance Device Manager displays the number of virtual contexts that can be supported using this resource class in the Maximum VC column. To support more or fewer virtual contexts, choose the resource class, click **Edit**, and modify it as described in this procedure.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.
- 

### Related Topics

- [Managing Resource Classes, page 4-35](#)
- [Modifying Resource Classes, page 4-40](#)

- [Deleting Resource Classes, page 4-41](#)
- [Viewing Resource Class Use on Virtual Contexts, page 4-41](#)

## Modifying Resource Classes

**Note**

This functionality is available for only Admin contexts.

When you modify a resource class, the ACE Appliance Device Manager applies the changes to virtual contexts that are associated with the resource class going forward. The changes are applied to existing virtual contexts already associated with the resource class.

**Caution**

If you allocate 100% of the resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost. For more information, see the [“Resource Allocation Constraints” section on page 4-36](#).

Use this procedure to modify an existing resource class.

**Note**

You cannot modify the default resource class.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > *admin context* > System > Resource Class**.  
The Resource Classes table appears.
- Step 2** Choose the resource class you want to modify, and then click **Edit**.  
The Edit Resource Class configuration screen appears.
- Step 3** Modify the fields as desired.  
For details on setting values, see the [“Adding Resource Classes” section on page 4-38](#). For descriptions of the resources, see [Table 4-10](#).
- Step 4** When you finish allocating the resources for this resource class, do one of the following:
  - Click **Deploy Now** to deploy this configuration on the ACE appliance. The configuration screen refreshes and the Max. Provisionable field beneath the Name field indicates the number of virtual contexts that can be supported using this resource allocation. When you are satisfied with the resource allocation and have saved your entries, click **Cancel** to return to the Resource Classes table.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

The ACE Appliance Device Manager applies all changes to the virtual contexts that use this resource class.

### Related Topics

- [Managing Resource Classes, page 4-35](#)

- [Adding Resource Classes, page 4-38](#)
- [Modifying Resource Classes, page 4-40](#)
- [Deleting Resource Classes, page 4-41](#)
- [Viewing Resource Class Use on Virtual Contexts, page 4-41](#)

## Deleting Resource Classes

**Note**

This functionality is available for only Admin contexts.

Use this procedure to remove resource classes from the ACE Appliance Device Manager database.

**Note**

When you remove a resource class from the ACE Appliance Device Manager, any virtual contexts that were associated with this resource class automatically become members of the default resource class. The default resource class allocates a minimum of 0.00% to a maximum of 100.00% of all ACE appliance resources to each context. You cannot modify the default resource class.

Because of the impact of resource class deletion on virtual contexts, we recommend that you view a resource class's current deployment before deleting it. See the [“Viewing Resource Class Use on Virtual Contexts” section on page 4-41](#).

### Procedure

- Step 1** Choose **Config > Virtual Contexts > *admin context* > System > Resource Class**.  
The Resource Classes table appears.
- Step 2** Choose the resource class you want to remove, and then click **Delete**.  
A window appears, asking you to confirm the deletion.
- Step 3** Click **OK** to continue deleting the resource class or click **Cancel** to keep the resource class.  
The Resource Classes table refreshes with the updated information.

### Related Topics

- [Managing Resource Classes, page 4-35](#)
- [Adding Resource Classes, page 4-38](#)
- [Modifying Resource Classes, page 4-40](#)
- [Viewing Resource Class Use on Virtual Contexts, page 4-41](#)

## Viewing Resource Class Use on Virtual Contexts

**Note**

This functionality is available for only Admin contexts.

Use this procedure to view a list of all virtual contexts using a selected resource class.

#### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > *admin context* > System > Resource Class**.
- The Resource Classes table lists the number of virtual contexts using each resource class in the second column.
- Step 2** Choose the resource class whose usage you want to view and then click **Virtual Contexts**.
- The Virtual Contexts Using Resource Class table appears, listing the associated contexts.
- Step 3** Click **Cancel** to return to the Resource Classes table.
- 

#### Related Topics

- [Managing Resource Classes, page 4-35](#)
- [Adding Resource Classes, page 4-38](#)
- [Modifying Resource Classes, page 4-40](#)
- [Deleting Resource Classes, page 4-41](#)
- [Viewing Resource Class Use on Virtual Contexts, page 4-41](#)

## Setting Resource Usage Thresholds to Receive SNMP Notifications

You can configure the ACE to issue SNMP traps and syslog messages when the resource usage by the ACE or a specific context breaches the specified thresholds (high, low, and watermark) for monitored resources listed in [Table 4-11](#).

**Table 4-11** *Monitored Resources with the Virtual Context*

| Resources                     | Virtual Context                                                                                                                                                                                       |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System bandwidth              | Admin                                                                                                                                                                                                 |
| System concurrent connections | Admin                                                                                                                                                                                                 |
| System connection rate        | Admin                                                                                                                                                                                                 |
| System active SSL connections | Admin                                                                                                                                                                                                 |
|                               | <b>Note</b> This resource option is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2). |
| System CPU utilization        | Admin                                                                                                                                                                                                 |
| System memory utilization     | Admin                                                                                                                                                                                                 |
| Bandwidth                     | All                                                                                                                                                                                                   |

**Table 4-11** *Monitored Resources with the Virtual Context*

| Resources              | Virtual Context |
|------------------------|-----------------|
| Concurrent connections | All             |
| Connection rate        | All             |

For each resource, you can specify the high, low, and watermark thresholds, which operate as follows:

- **High**—Indicates the highest value of the threshold defined. This value is configured as a percentage between 1 to 100 and is represented as the highest percentage of the maximum number of allocated resources. The ACE sends a notification/trap to the SNMP when the current resource usage exceeds the highest threshold value.
- **Low**—Indicates the lowest value of the threshold defined. This value is configured as a percentage between 1 to 100 and is represented as the lowest percentage of the minimum number of allocated resources. The ACE sends a notification/trap to the SNMP when the current resource usage is less than the specified lowest threshold value.



**Note** You cannot set a lower limit for active SSL connections, CPU utilization, and memory utilization because there is no lower limit imposed on these resources.

- **Watermark**—Indicates the defined watermark threshold. A watermark is configured as a percentage between 1 to 100 and is represented as the percentage of the maximum and minimum allocated resource, which operates as follows:
  - **High watermark**—The ACE sends a Falling Watermark notification when the current resource usage level exceeds the high watermark value.
  - **Low watermark**—The ACE sends a Rising Watermark notification when the current resource usage level is below the low watermark value.

#### Prerequisites

- The context is configured for SNMP (see the [“Configuring SNMP for Virtual Contexts”](#) section on page 4-19).
- A resource class is configured and associated with the context (see the [“Managing Resource Classes”](#) section on page 4-35).

#### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > System > Resource Usage Threshold**.  
The Resource Usage Threshold window appears.
- Step 2** From the Resource Usage Threshold window, specify the high, low, and watermark percentages.  
Enter the percentage values using the following guide:  
1 <= Low < Watermark < High <= 100 (percent)  
Decimal values are not allowed.
- Step 3** Click **Deploy Now**.
-

**Related Topics**

- [Configuring the Resource Usage Threshold for Real Server, page 4-44](#)
- [Configuring the Resource Usage Threshold for VIP, page 4-45](#)
- [Configuring SNMP for Virtual Contexts, page 4-19](#)
- [Managing Resource Classes, page 4-35](#)

## Configuring the Resource Usage Threshold for Real Server

You can configure the ACE to issue SNMP traps and syslog messages at the real server level for the following monitored resources:

- **Bandwidth**—Thresholds are applied to the aggregated bandwidth for a particular real server.
- **Concurrent connections**—Thresholds are applied to the aggregated concurrent connections for a particular real server.
- **Connection rate**—Thresholds are applied to the aggregated connection rate for a particular real server.

All the resources configured under the server farm are monitored at a particular real server level. For each resource, you can specify the high, low, and watermark thresholds.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > System > Resource Usage Threshold > Real Server Threshold**.
- The Real Server Threshold table appears.
- Step 2** Click **Add** to add a new real server threshold, or select a real server threshold you want to modify, and then click **Edit**. The Real Server Threshold screen appears.
- Step 3** In the **Real Server Name** field, enter the name of the real server that is associated with the selected server farm.
- Step 4** In the **Server Farm Name** field, enter the name of the server farm.
- Step 5** For each resource, specify the high, low, and watermark percentages.
- Enter the percentage values using the following guide:
- 1 <= Low < Watermark < High <= 100 (percent)
- Decimal values are not allowed.
- Step 6** Do one of the following:
- Click **Deploy Now**.
  - Click **Cancel** to exit this procedure without saving your selection and to return to the Real Server Threshold table.
  - Click **Add Another** to save your entries and to add another entry to the Real Server Threshold table. The screen refreshes and you can select another Real Server Threshold option.
- 

**Related Topics**

- [Configuring the Resource Usage Threshold for VIP, page 4-45](#)

- [Configuring SNMP for Virtual Contexts, page 4-19](#)
- [Managing Resource Classes, page 4-35](#)

## Configuring the Resource Usage Threshold for VIP

You can configure the ACE to issue SNMP traps and syslog messages for a VIP for the following monitored resources:

- Bandwidth—Thresholds are applied to the aggregated bandwidth for a particular VIP.
- Concurrent connections—Thresholds are applied to the aggregated concurrent connections for a particular VIP.
- Connection rate—Thresholds are applied to the aggregated connection rate for a particular VIP.

For each resource, you can specify the high, low, and watermark thresholds.

### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; System &gt; Resource Usage Threshold &gt; VIP Threshold</b> .                                                                                                                                                                                                                                                                |
|               | The VIP Threshold table appears.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 2</b> | Click <b>Add</b> to add a VIP threshold, or select a VIP threshold you want to modify, and then click <b>Edit</b> . The VIP Threshold screen appears.                                                                                                                                                                                                                                 |
| <b>Step 3</b> | In the <b>VIP Address</b> field, enter the virtual IP address.                                                                                                                                                                                                                                                                                                                        |
| <b>Step 4</b> | In the <b>Class Map Name</b> field, enter the name of the Layer 3/4 Network Traffic class map.                                                                                                                                                                                                                                                                                        |
| <b>Step 5</b> | In the <b>Policy Map Name</b> field, enter the name of the Layer 3/4 Network Traffic (Multi-Match) policy map.                                                                                                                                                                                                                                                                        |
| <b>Step 6</b> | For each resource, specify the high, low, and watermark percentages.<br><br>Enter the percentage values using the following guide:<br>1 <= Low < Watermark < High <= 100 (percent)<br><br>Decimal values are not allowed.                                                                                                                                                             |
| <b>Step 7</b> | Do one of the following: <ul style="list-style-type: none"><li>• Click <b>Deploy Now</b>.</li><li>• Click <b>Cancel</b> to exit this procedure without saving your selection and to return to the VIP table.</li><li>• Click <b>Add Another</b> to save your entries and to add another entry to the VIP table. The screen refreshes and you can select another VIP option.</li></ul> |
- 

### Related Topics

- [Configuring the Resource Usage Threshold for Real Server, page 4-44](#)
- [Configuring SNMP for Virtual Contexts, page 4-19](#)
- [Managing Resource Classes, page 4-35](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)

# Using the Configuration Checkpoint and Rollback Service

At some point, you may want to modify your ACE running configuration. If you run into a problem with the modified configuration, you may need to reboot your ACE. To prevent having to reboot your ACE after unsuccessfully modifying a running configuration, you can create a checkpoint (a snapshot in time) of a known stable running configuration before you begin to modify it. If you encounter a problem with the modifications to the running configuration, you can roll back the configuration to the previous stable configuration checkpoint.

**Note**

Before you upgrade your ACE software, we strongly recommend that you create a checkpoint in your running configuration. For software release A4(1.0), use the backup function to create a backup of the running configuration (see the [“Performing Device Backup and Restore Functions”](#) section on page 4-49).

The ACE allows you to make a checkpoint configuration at the context level. The ACE stores the checkpoint for each context in a hidden directory in Flash memory. If, after you make configuration changes that modify the current running configuration, when you roll back the checkpoint, the ACE causes the running configuration to revert to the checkpointed configuration.

This section includes the following topics:

- [Creating a Configuration Checkpoint, page 4-46](#)
- [Deleting a Configuration Checkpoint, page 4-47](#)
- [Rolling Back a Running Configuration, page 4-48](#)
- [Comparing the Checkpoint with the Running Configuration, page 4-48](#)
- [Displaying Checkpoint Information, page 4-49](#)

## Creating a Configuration Checkpoint

You can create a configuration checkpoint for a specific context. The ACE supports a maximum of 10 checkpoints for each context.

**Assumption**

This topic assumes the following:

- Make sure that the current running configuration is stable and is the configuration that you want to make as a checkpoint. If you change your mind after creating the checkpoint, you can delete it (see the [“Deleting a Configuration Checkpoint”](#) section on page 4-47).
- The ACE-Admin, DM-Admin, and Org-Admin predefined roles have access to the configuration checkpoint function.
- A custom role with the Device Manager Inventory and Virtual Context role tasks set to create or modify has the required privileges to create a configuration checkpoint.
- A checkpoint will not include the SSL keys/certificates, probe scripts, and licenses.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.
- Adding a checkpoint from an ACE context directly will not trigger an autosynchronization on the ACE Appliance Device Manager for that context.



### Procedure

- Step 1** Choose **Config > Virtual Contexts > admin context > System > Checkpoints**.

The Checkpoints table appears.

For descriptions of the checkpoints, see [Table 4-12](#).

**Table 4-12** Checkpoints Table

| Field             | Description                                           |
|-------------------|-------------------------------------------------------|
| Name              | Unique identifier of the checkpoint.                  |
| Size (In Bytes)   | Size of the configuration checkpoint, shown in bytes. |
| Date (Created On) | Date that the configuration checkpoint was created.   |

- Step 2** In the Checkpoints table, click **Create Checkpoint**.

The Create Checkpoint dialog box appears.

- Step 3** In the Checkpoint Name field of the Create Checkpoint dialog box, specify a unique identifier for the checkpoint.

Enter a text string with no spaces and a maximum of 25 alphanumeric characters.

If the checkpoint already exists, you are prompted to use a different name.

- Step 4** Do one of the following:

- Click **OK** to save your configuration checkpoint. You return to the Checkpoints table and the new checkpoint appears in the table.
- Click **Cancel** to exit the procedure without saving the configuration checkpoint and to return to the Checkpoints table.

## Deleting a Configuration Checkpoint

You can delete a checkpoint. Deleting a checkpoint from an ACE context directly will not trigger an autosynchronization to occur on the ACE Appliance Device Manager for that context.

### Prerequisite

Before you perform this procedure, make sure that you want to delete the checkpoint. Once you click the Trash icon, the ACE removes the checkpoint from Flash memory.

This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

### Procedure

- Step 1** To choose a virtual context that you want to create a configuration checkpoint, choose **Config > Virtual Contexts > admin context > System > Checkpoints**.

The Checkpoints table appears.

- Step 2** In the Checkpoints table, choose the radio button to the left of any table entry, and click the **Trash** icon to delete the checkpoint.
- 

## Rolling Back a Running Configuration

You can roll back the current running configuration of a context to the previously checkpointed running configuration.



**Note** This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

---

### Procedure

---

- Step 1** Choose **Config > Virtual Contexts > admin context > System > Checkpoints**.  
The Checkpoints table appears.
- Step 2** Choose the radio button to the left of the checkpoint that you wish to roll back, and click **Rollback**.  
The ACE Appliance Device Manager displays a confirmation popup window to warn you about this change and to instruct you that the rollback operation may take longer depending on the differences detected between the two configurations.



**Note** The ACE Appliance Device Manager synchronizes the device after performing a rollback. This synchronization may take some time.

---

## Comparing the Checkpoint with the Running Configuration

You can compare an existing checkpoint with the running configuration.

### Procedure

---

- Step 1** Choose **Config > Virtual Contexts > admin context > System > Checkpoints**.  
The Checkpoints table appears.
- Step 2** In the Checkpoints table, choose the radio button to the left of the checkpoint that you want to compare, and click **Compare**.  
The ACE Appliance Device Manager uses the ACE **compare checkpoint\_name** CLI command to compare the running configuration of the specified checkpoint.  
If the checkpoint configuration is the same as the running-config, the output of this command is as follows:  

```
Checkpoint config is same as running config
```

If the checkpoint configuration is different from the running-config, the output will be the difference between the two configurations. The items in red are in the current running configuration and will be removed. The items in green are not in the current running configuration and will be added.

**Step 3** Click **Close** to exit the dialog box and return to the Checkpoints table.

---

## Displaying Checkpoint Information

You can display checkpoint information.

### Procedure

---

**Step 1** Choose **Config > Virtual Contexts > admin context > System > Checkpoints**.

The Checkpoints table appears.

**Step 2** In the Checkpoints table, choose the radio button to the left of the checkpoint that you want to display, and click **Details**.

The ACE Appliance Device Manager uses the ACE **show checkpoint detail {name}** CLI command to display the running configuration of the specified checkpoint.

**Step 3** Click **Close** to exit the dialog box and return to the Checkpoints table.

---

## Performing Device Backup and Restore Functions

The backup and restore functions allow you to back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context. Configuration dependencies are those files that are required to exist on the ACE so that a configuration can be applied to it. Such files include health-monitoring scripts, SSL certificates, SSL keys, and so on.



### Note

This section includes information about backing up and restoring SSL files, which is not applicable with the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

---

This feature allows you to back up and restore the following configuration files and dependencies:

- Running-configuration files
- Startup-configuration files
- Checkpoints
- SSL files (SSL certificates and keys)
- Health-monitoring scripts
- Licenses

**Note**


---

The backup feature does not back up the sample SSL certificate and key pair files.

---

Typical uses for this feature are as follows:

- Back up a configuration for later use
- Recover a configuration that was lost because of a software failure or user error
- Restore configuration files to a new ACE when a hardware failure resulted in a Return Merchandise Authorization (RMA) of the old ACE
- Transfer the configuration files to a different ACE

The backup and restore functions are supported in both the Admin and virtual contexts. If you perform these functions in the Admin context, you can back up or restore the configuration files for either the Admin context only or for all contexts in the ACE. If you perform these functions in a virtual context, you can back up or restore the configuration files only for that context. Both the backup and the restore functions run asynchronously (in the background).

### Archive Naming Conventions

Context archive files have the following naming convention format:

*Hostname\_ctxname\_timestamp.tgz*

The filename fields are as follows:

- *Hostname*—Name of the ACE. If the hostname contains special characters, the ACE uses the default hostname “switch” in the filename. For example, if the hostname is Active@~!#\$%^, then the ACE assigns the following filename: switch\_Admin\_2009\_08\_30\_15\_45\_17.tgz
- *ctxname*—Name of the context. If the context name contains special characters, the ACE uses the default context name “context” in the filename. For example, if the context name is Test!123\*, then the ACE assigns the following filename: switch\_context\_2009\_08\_30\_15\_45\_17.tgz
- *timestamp*—Date and time that the ACE created the file. The time stamp has the following 24 hour format: YYYY\_MM\_DD\_hh\_mm\_ss

An example is as follows:

ACE-1\_ctx1\_2009\_05\_06\_15\_24\_57.tgz

If you back up the entire ACE, the archive filename does not include the *ctxname* field. So, the format is as follows:

*Hostname\_timestamp.tgz*

An example is as follows:

ACE-1\_2009\_05\_06\_15\_24\_57.tgz

### Archive Directory Structure and Filenames

The ACE uses a flat directory structure for the backup archive. The ACE provides file extensions for the individual files that it backs up so that you can identify the types of files easily when restoring an archive. All files are stored in a single directory that is tarred and GZIPed as follows:

```
ACE-1_Ctx1_2009_05_06_07_24_57.tgz
ACE-1_Ctx1_2009_05_06_07_24_57\
 context_name-running
 context_name-startup
 context_name-chkpt_name.chkpt
```

```
context_name-cert_name.cert
context_name-key_name.key
context_name-script_name.tcl
context_name-license_name.lic
```

### Guidelines and Limitations

The backup and restore functions have the following configuration guidelines and limitations:

- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.
- Store the backup archive on disk0: in the context of the ACE where you intend to restore the files. Use the Admin context for a full backup and the corresponding context for user contexts.
- When you back up the running-configuration file, the ACE uses the output of the **show running-configuration** CLI command as the basis for the archive file.
- The ACE backs up only exportable certificates and keys.
- License files are backed up only when you back up the Admin context.
- Use a pass phrase to back up SSL keys in encrypted form. Remember the pass phrase or write it down and store it in a safe location. When you restore the encrypted keys, the ACE prompts you for the pass phrase to decrypt the keys. If you do not use a pass phrase when you back up the SSL keys, the ACE restores the keys with AES-256 encryption using OpenSSL software.
- Only probe scripts that reside in disk0: need to be backed up. The prepackaged probe scripts in the probe: directory are always available. When you perform a backup, the ACE automatically identifies and backs up the scripts in disk0: that are required by the configuration.
- The ACE does not resolve any other dependencies required by the configuration during a backup except for scripts that reside in disk0:. For example, if you configured SSL certificates in an SSL proxy in the running-configuration file, but you later deleted the certificates, the backup proceeds anyway as if the certificates still existed.
- To perform a restore operation, you must have the admin RBAC feature in your user role. DM-admin and ORG-admin have access to this feature by default. Custom roles with the Device Manager Inventory and Virtual Context role tasks set to create or modify can also access this feature.
- When you instruct the ACE to restore the archive for the entire ACE, it restores the Admin context completely first, and then it restores the other contexts. The ACE restores all dependencies before it restores the running configuration. The order in which the ACE restores dependencies is as follows:
  - License files
  - SSL certificates and key files
  - Health-monitoring scripts
  - Checkpoints
  - Startup-configuration file
  - Running-configuration file
- When you restore the ACE, previously installed license files are uninstalled and the license files in the backup file are installed in their place.
- In a redundant configuration, if the archive that you want to restore is different from the peer configurations in the FT group, redundancy may not operate properly after the restore.
- You can restore a single context from a full backup archive provided that you do the following:
  - You execute the restore operation in the context that you want to restore

- All files dependencies for the context exist in the full backup archive
- To enable the ACE Device Manager to synchronize the CLI after a successful restore, do not navigate from the Backup / Restore page until the Latest Restore status changes from In Progress to Success. If you navigate to another page before the restore process is complete, the CLI will not synchronize until you return to the Backup / Restore page or until the automatic or manual CLI CLI synchronization occurs.

### Defaults

Table 4-13 lists the default settings for the backup and restore function parameters.

**Table 4-13**      *Default Backup and Restore Parameters*

| Parameter                  | Default                                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backed up files            | By default the ACE backs up the following files in the current context: <ul style="list-style-type: none"> <li>• Running-configuration file</li> <li>• Startup-configuration file</li> <li>• Checkpoints</li> <li>• SSL certificates</li> <li>• SSL keys</li> <li>• Health-monitoring scripts</li> <li>• Licenses</li> </ul> |
| SSL key restore encryption | None                                                                                                                                                                                                                                                                                                                         |

This section includes the following topics:

- [Backing Up Device Configuration and Dependencies, page 4-52](#)
- [Restoring Device Configuration and Dependencies, page 4-55](#)

## Backing Up Device Configuration and Dependencies

You can create a backup of an ACE configuration and its dependencies.



### Note

When you perform the backup process from the Admin context, you can either back up the Admin context files only or you can back up the Admin context and all user contexts. When you back up from a user context, you back up the current context files only and cannot back up the ACE licenses.



### Note

If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

### Procedure

- Step 1**      Choose **Config > Virtual Contexts > System > Backup / Restore**.

The Backup / Restore table appears and displays the latest backup and restore statistics.



**Note** To refresh the table content at any time, click **Poll Now**.



**Note** When you choose the Backup / Restore operation, the Appliance Device Manager must poll a context if that context has not been accessed previously for this operation. The polling operation, which is necessary to obtain the latest backup and restore information, can cause a delay in the display time of the Backup / Restore table.

The Backup / Restore fields are described in [Table 4-14](#).

**Table 4-14 Backup / Restore Fields**

| Field                 | Description                                                                                                                                                                                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Latest Backup</b>  |                                                                                                                                                                                                                                                                                                                |
| Backup Archive        | Name of the last *.tgz file created that contains the backup files.                                                                                                                                                                                                                                            |
| Type                  | Type of backup: Context or Full (all contexts).                                                                                                                                                                                                                                                                |
| Start-time            | Date and time that the last backup began.                                                                                                                                                                                                                                                                      |
| Finished-time         | Date and time that the last backup ended.                                                                                                                                                                                                                                                                      |
| Status                | Status of the last context to be backed up: Success, In Progress, or Failed. Click the status link to view status details.                                                                                                                                                                                     |
| Current vc            | Name of the last context in the backup process.                                                                                                                                                                                                                                                                |
| Completed             | Number of context backups completed compared to the total number of context backup requests.<br>For example: <ul style="list-style-type: none"> <li>2/2 = Two context backups completed/Two context backups requested</li> <li>0/1 = No context backup completed/One context backup requested</li> </ul>       |
| <b>Latest Restore</b> |                                                                                                                                                                                                                                                                                                                |
| Backup Archive        | Name of the *.tgz file used in during the restore process.                                                                                                                                                                                                                                                     |
| Type                  | Type of restore: Context or Full (all contexts).                                                                                                                                                                                                                                                               |
| Start-time            | Date and time that the last restore began.                                                                                                                                                                                                                                                                     |
| Finished-time         | Date and time that the last restore ended.                                                                                                                                                                                                                                                                     |
| Status                | Status of the last restore: Success, In Progress, or Failed. Click the status to view status details.                                                                                                                                                                                                          |
| Current vc            | Name of the last context in the restore process.                                                                                                                                                                                                                                                               |
| Completed             | Number of context restores completed compared to the total number of context restore requests.<br>For example: <ul style="list-style-type: none"> <li>2/2 = Two context restores completed/Two context restores requested</li> <li>0/1 = No context restore completed/One context restore requested</li> </ul> |

**Step 2 Click Backup.**

The Backup window appears.

- Step 3** In the Backup window, click the radio button of the location where the ACE is to save the backup files:
- **Backup config on ACE (disk0:)**—This is the default. Go to Step 9.
  - **Backup config on ACE (disk0:) and then copy to remote system**—The Remote System attributes step appears. Go to Step 4.
- Step 4** Click the radio button of the transfer protocol to use:
- **FTP**—File Transfer Protocol
  - **SFTP**—Secure File Transfer Protocol
  - **TFTP**—Trivial File Transfer Protocol
- Step 5** In the Username field, enter the username that the remote server requires for user authentication. This field appears for FTP and SFTP only.
- Step 6** In the Password field, enter the password that the remote server requires for user authentication. This field appears for FTP and SFTP only.
- Step 7** In the IP Address field, enter the IP address of the remote server.
- Step 8** In the Backup File Path in Remote System field, enter the full path for the remote server.
- Step 9** Check the **Backup All Contexts** check box if you want the ACE to create a backup that contains the files of the Admin context and every user context or uncheck the check box to create a backup of the Admin context files only. This field appears for the Admin context only.
- Step 10** Indicate the components to exclude from the backup process: Checkpoints or SSL Files.

**Note**

The SSL Files option is not available for the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

To exclude a component, double-click on it in the Available box to move it to the Selected box. You can also use the right and left arrows to move selected items between the two boxes.

**Caution**

If you exclude the SSL Files component and then restore the ACE using this archived backup, these files are removed from the ACE. To save these files prior to performing a restore with this backup, use the **crypto export** CLI command to export the keys to a remote server and use the **copy** CLI command to copy the license files to disk0: as .tar files.

- Step 11** In the Pass Phrase field, enter the pass phrase that you specify to encrypt the backed up SSL keys.

**Note**

This field is not available with the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

Enter the pass phrase as an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. If you enter a pass phrase but exclude the SSL files from the archive, the ACE does not use the pass phrase.

- Step 12** Click **OK** to begin the backup process.

The following actions occur depending on where the ACE Device Manager saves the files:



- **disk0: only**—The Device Manager permits continued GUI functionality during the backup process and polls the ACE for the backup status, which it displays on the Backup / Restore page.
- **disk0: and a remote server**—The Device Manager suspends GUI operation and displays a “Please Wait” message in the Backup dialog box until the process is complete. During this process, the ACE Device Manager instructs the ACE to create and save the backup file locally to disk0: and then place a copy of the file on the specified remote server.

**Step 13** In the Backup / Restore page, click **Poll Now** to ensure that the latest backup statistics are displayed, and then click on the Status link (**Success**, **In Progress**, or **Failed**) located in the Latest Backup column to view details of the backup operation.

If the backup status is either Success or In Progress, then the Show Backup Status Detail pop-up window appears and displays a list of the files successfully backed up. When the backup status is In Progress, the ACE Device Manager polls the ACE every 2 minutes to retrieve the latest status information and then it automatically updates the status information displayed. The polling continues until the ACE Device Manager receives a status of either Success or Failed. If the backup status is Failed, then the Show Backup Errors popup window appears, displaying the reason for the failed backup attempt.

#### Related Topics

- [Restoring Device Configuration and Dependencies, page 4-55](#)

## Restoring Device Configuration and Dependencies

You can restore an ACE configuration and its dependencies using a backup file.



#### Caution

The restore operation clears any existing SSL certificate and key-pair files, license files, and checkpoints in a context before it restores the backup archive file. If your configuration includes SSL files or checkpoints and you excluded them when you created the backup archive, those files will no longer exist in the context after you restore the backup archive. To preserve any existing exportable SSL certificate and key files in the context, before you execute the restore operation, export the certificates and keys that you want to keep to an FTP, SFTP, or TFTP server by using the CLI and the **crypto export** command. After you restore the archive, import the SSL files into the context. For details on exporting and importing SSL certificate and key pair files using the CLI, see the *SSL Guide, Cisco ACE Application Control Engine*.

You can also use the exclude option of the restore command to instruct the ACE not to clear the SSL files in disk0: and to ignore the SSL files in the backup archive when the ACE restores the backup.

Ignore this Caution if the ACE is using the NPE software version, which does not allow encryption protocols (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2)



#### Note

If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

**Prerequisites**

If you are going to restore the Admin context files plus all user context files, use a backup file that was created from the Admin context with the Backup All Contexts check box checked (see the “[Backing Up Device Configuration and Dependencies](#)” section on page 4-52).

**Procedure**

**Step 1** Choose **Config > Virtual Contexts > System > Backup / Restore**.

The Backup / Restore table appears.



**Note** To refresh the table content at any time, click **Poll Now**.



**Note** When you perform the restore process from the Admin context, you can either restore the Admin context files only or you can restore the Admin context files plus all user context files. When you perform the restore process from a user context, you can restore the current context files only.

The Backup / Restore fields are described in [Table 4-14](#).

**Step 2** Click **Restore**.

The Restore window appears.



**Note** The display of the Restore window may be delayed because the Device Manager is retrieving the list of the disk0: archive (\*.tgz) files.

**Step 3** In the Restore window, click the desired radio button to specify the location where the backup files are located saved:

- **Choose a backup file on the ACE (disk0:)**—This is the default. Go to Step 9.
- **Choose a backup file from remote system**—The Remote System attributes step appears. Go to Step 4.

**Step 4** Click the radio button of the transfer protocol to use:

- **FTP**—File Transfer Protocol
- **SFTP**—Secure File Transfer Protocol
- **TFTP**—Trivial File Transfer Protocol

**Step 5** In the Username field, enter the username that the remote file system requires for user authentication. This field appears for FTP and SFTP only.

**Step 6** In the Password field, enter the password that the remote file system requires for user authentication. This field appears for FTP and SFTP only.

**Step 7** In the IP Address field, enter the IP address of the remote server.

**Step 8** In the Backup File Path in Remote System field, enter the full path of the backup file, including the backup filename, to be copied from the remote server.

**Step 9** Check the **Restore All Contexts** check box if you want the ACE to restore the files for every context or uncheck the check box to restore the Admin context files only.

This field appears for the Admin context only.

- Step 10** Check the **Exclude SSL Files** check box if you want to preserve the SSL files currently loaded on the ACE and not use the backup file's SSL files.



**Note** This check box is not available with the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).



**Caution** The restore function deletes all SSL files currently loaded on the ACE unless you check the Exclude SSL Files option. If you do not check this option, the restore function loads the SSL files included in the backup file. If the backup file does not include SSL files, the ACE will not have any SSL files loaded on it when the restore process is complete. You will then need to import copies of the SSL files from a remote server.

- Step 11** In the Pass Phrase field, enter the pass phrase that is used to encrypt the backed up SSL keys in the archive.



**Note** This field is not available with the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

Enter the pass phrase as an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. The Pass Phrase field does not appear when you check the Exclude SSL Files check box.

- Step 12** Click **OK** to begin the restore process.

The following actions occur depending on where the ACE Device Manager retrieves the backup files:

- **disk0:** only—The ACE Device Manager permits continued GUI functionality during the restore process and polls the ACE for the backup status, which it displays on the Backup / Restore page.



**Note** To enable the Device Manager to synchronize the CLI after a successful restore, do not navigate from the Backup / Restore window until the Latest Restore status changes from In Progress to Success. If you navigate to another window before the restore process is complete, the CLI will not synchronize until you return to the Backup / Restore window or until the automatic or manual CLI synchronization occurs.

- **disk0:** and a remote server—The ACE Device Manager suspends GUI operation and displays a “Please Wait” message in the Restore dialog box until the process is complete. During this process, the ACE Device Manager instructs the ACE to copy the backup file from the specified remote server to disk0: on the ACE and then apply the backup file to the context.

- Step 13** In the Backup / Restore page, click **Poll Now** to ensure that the latest restore statistics are displayed, and then click on the Status link (**Success**, **In Progress**, or **Failed**) located in the Latest Backup column to view details of the restore operation.

If the restore status is either Success or In Progress, then the Show Restore Status Detail popup window appears and displays a list of the files successfully restored. When the restore status is In Progress, the ACE Device Manager polls the ACE every 2 minutes to retrieve the latest status information and then it

automatically updates the status information displayed. The polling continues until the ACE Device Manager receives a status of either Success or Failed. If the restored status is Failed, then the Show Restored Errors popup window appears, displaying the reason for the failed restore attempt.

---

#### Related Topics

- [Performing Device Backup and Restore Functions, page 4-49](#)

## Configuring Security with ACLs

An ACL (access control list) consists of a series of statements called ACL entries that collectively define the network traffic profile. Each entry permits or denies network traffic (inbound and outbound) to the parts of your network specified in the entry. Besides an action element (“permit” or “deny”), each entry also contains a filter element based on criteria such as source address, destination address, protocol, or protocol-specific parameters. An implicit “deny all” entry exists at the end of every ACL, so you must configure an ACL on every interface where you want to permit connections. Otherwise, the ACE denies all traffic on the interface.

ACLs provide basic security for your network by allowing you to control network connection setups rather than processing each packet. Such ACLs are commonly referred to as *security ACLs*.

You can configure ACLs as parts of other features; for example, security, network address translation (NAT), or server load balancing (SLB). The ACE merges these individual ACLs into one large ACL called a *merged ACL*. The ACL compiler then parses the merged ACL and generates the ACL lookup mechanisms. A match on this merged ACL can result in multiple actions. You can add, modify, or delete entries to an ACL already in the summary table, or add a new ACL to the list.

When you use ACLs, you may want to permit all e-mail traffic on a circuit, but block FTP traffic. You can also use ACLs to allow one client to access a part of the network and prevent another client from accessing that same area.

When configuring ACLs, you must apply an ACL to an interface to control traffic on that interface. Applying an ACL on an interface assigns the ACL and its entries to that interface.

You can apply only one extended ACL to each direction (inbound or outbound) of an interface. You can also apply the same ACL on multiple interfaces. You can apply EtherType ACLs in only the inbound direction and on only Layer 2 interfaces.



#### Note

By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

---

This section contains the following topics:

- [Creating ACLs, page 4-59](#)
- [Setting EtherType ACL Attributes, page 4-67](#)
- [Setting Extended ACL Attributes, page 4-61](#)
- [Resequencing Extended ACLs, page 4-66](#)
- [Viewing All ACLs by Context, page 4-68](#)
- [Editing or Deleting ACLs, page 4-69](#)

## Creating ACLs


**Note**

By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

Use this procedure to create, modify, or delete ACLs.

**Procedure**

**Step 1** Choose **Config > Virtual Contexts > context > Security > ACLs**.

The ACL summary table appears, listing the existing ACLs. ACL summary fields are described in [Table 4-15](#).

**Table 4-15** *ACL Summary Table*

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | Enter a unique identifier for the ACL. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Type            | Specifies the type of ACL: <ul style="list-style-type: none"> <li>Extended—This ACL allows you to specify both the source and the destination IP addresses of traffic as well as the protocol and the action to be taken. For more information, see the <a href="#">“Setting Extended ACL Attributes”</a> section on page 4-61.</li> <li>Ethertype—This ACL controls network access for non-IP traffic based on its EtherType. An EtherType is a sub-protocol identifier. For more information, see the <a href="#">“Setting EtherType ACL Attributes”</a> section on page 4-67.</li> </ul> |
| IP Address Type | Specifies the type of IP address: <ul style="list-style-type: none"> <li>IPv4—This ACL controls network access for IPv4 traffic.</li> <li>IPv6—This ACL controls network access for IPv6 traffic.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |
| # (Line Number) | ACL line number for extended type ACL entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Action          | Action to be taken (permit/deny).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Protocol        | Protocol number or service object group to apply to this ACL entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Source          | Source IPv6 or IPv4 address or source network object group (if configured) that is being applied to this ACL entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Destination     | Destination IPv6 or IPv4 address or destination network object group (if configured) that is applied to this ACL entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ICMP            | Indicates whether or not this ACL uses ICMP (Internet Control Message Protocol). For more information, see the <a href="#">“Table 4-18 Protocol Names and Numbers”</a> section on page 4-64.                                                                                                                                                                                                                                                                                                                                                                                                |

**Table 4-15** *ACL Summary Table (continued)*

| Field     | Description                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface | VLAN interface(s) that is/are associated with this ACL, for example in4,5:4out where, in denotes the input direction, out denotes the output direction.                                                                                      |
| Remark    | Enter any comments you want to include for this ACL. Valid entries are unquoted text strings with a maximum of 100 characters. You can enter leading spaces at the beginning of the text or special characters. Trailing spaces are ignored. |

**Step 2** From the summary table, do one of the following:

- To view full details of an ACL inline, click the plus sign to the left of any table entry.
- To create an ACL, click the **Add** icon. The New Access List screen appears (go to [Step 3](#)).
- To modify an ACL, select the radio button to the left of any table entry, and then click the **Edit** icon. The Edit ACL or Edit ACL entry screen appears based on the selected radio button to the left of any table entry (go to [Step 3](#)).
- To delete an ACL, select the radio button to the left of any table entry, and then click the **Delete** icon.

**Step 3** Add or edit required fields as described in [Table 4-16](#).

**Table 4-16** *ACL Configuration Attributes*

| Field                    | Description                                                                                                                                                                                                                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACL Properties           | Includes name, type (Extended, Ethertype), IP address type (IPv6 and IPv4), and remarks. For more information, see the “ <a href="#">Table 4-15 ACL Summary Table</a> ” task on page 4-59.                                                                                                                                         |
| <b>ACL Entries</b>       |                                                                                                                                                                                                                                                                                                                                    |
| Entry Attributes         | Includes line number, action (Permit, Deny), protocol or service object group, and associated drop down descriptor menu. For more information for these attributes, see the “ <a href="#">Setting Extended ACL Attributes</a> ” section on page 4-61 or “ <a href="#">Setting EtherType ACL Attributes</a> ” section on page 4-67. |
| Source                   | (Extended type ACL only) Source IPv6 address and prefix length, IPv4 address and netmask with port number (if configured), or network object group (if configured) that is being applied to this ACL entry. For more information see the “ <a href="#">Setting Extended ACL Attributes</a> ” section on page 4-61.                 |
| Destination              | (Extended type ACL only) Destination IPv6 address and prefix length, IPv4 address and netmask with port number (if configured), or network object group (if configured) that is being applied to this ACL entry. For more information see the “ <a href="#">Setting Extended ACL Attributes</a> ” section on page 4-61.            |
| Add To Table button      | Used to add multiple ACL entries, adding one at a time using this button, before clicking <b>Deploy</b> . In the past only one entry could be added at a time in a two-step process hopping between two different locations in the UI.                                                                                             |
| Remove From Table button | Used to remove multiple ACL entries, removing one at a time using this button, before clicking <b>Deploy</b> .                                                                                                                                                                                                                     |

Table 4-16 ACL Configuration Attributes (continued)

| Field                                                                                                                | Description                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Interfaces</b>                                                                                                    |                                                                                                                                                                                                                                                       |
| <ul style="list-style-type: none"> <li>Input/Output Direction</li> <li>Currently Assigned (ACL:Direction)</li> </ul> | Allows you to associate the ACL with one or more interfaces allowing only one input and one output ACL for each interface. The top left check box under the Interfaces section allows you to select and apply to all interfaces “access-group input.” |



**Note** To add, modify, or delete Object Groups, see the [“Configuring Object Groups” section on page 4-70](#).

- Step 4** Do one of the following:
- Click **Deploy** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the ACLs table.

#### Related Topics

- [Configuring Security with ACLs, page 4-58](#)
- [Setting EtherType ACL Attributes, page 4-67](#)
- [Setting Extended ACL Attributes, page 4-61](#)
- [Resequencing Extended ACLs, page 4-66](#)
- [Editing or Deleting ACLs, page 4-69](#)

## Setting Extended ACL Attributes



**Note** By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

An extended ACL allows you to specify both the source and the destination IP addresses of traffic as well as the protocol and the action to be taken.

For TCP, UDP, and ICMP connections, you do not need to also apply an ACL on the destination interface to allow returning traffic, because the ACE allows all returning traffic for established connections.



**Note** The ACE does not explicitly support standard ACLs. To configure a standard ACL, specify the destination address as **any** and do not specify the ports in an extended ACL.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Security > ACLs**.
- The ACLs table appears, listing the existing ACLs.

- Step 2** Click **Add**. The New Access List configuration screen appears.
- Step 3** Enter the ACL name in the ACL Properties pane and choose the type as Extended.  
Choose the IP Address Type as either IPV6 or IPv4.
- Step 4** Configure extended ACL entries using the information in [Table 4-17](#).

**Table 4-17**      *Extended ACL Configuration Options*

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Entry Attributes</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Line Number             | Enter a number that specifies the position of this entry in the ACL. The position of an entry affects the lookup order of the entries in an ACL. To change the sequence of existing extended ACLs, see the <a href="#">“Resequencing Extended ACLs”</a> section on page 4-66.                                                                                                                                                                                                                                                                                                                                                                               |
| Action                  | Action to be taken (permit/deny).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Service Object Group    | Select a service object group to apply to this ACL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Protocol                | Select the protocol or protocol number to apply to this ACL entry. <a href="#">Table 4-18</a> lists common protocol names and numbers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ICMP Type               | Select the ICMP type or number for this protocol. <ul style="list-style-type: none"> <li><a href="#">Table 4-19</a> lists common ICMP types and numbers, per RFC 792.</li> <li><a href="#">Table 4-20</a> lists the common ICMPv6 types and associated numbers, per RFC 4443.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| Message Code Operator   | Choose the operand to use when comparing message codes for this service object: <ul style="list-style-type: none"> <li>Equal To—The message code must be the same as the number in the Message Code field.</li> <li>Greater Than—The message code must be greater than the number in the Message Code field.</li> <li>Less Than—The message code must be less than the number in the Message Code field.</li> <li>Not Equal To—The message code must not equal the number in the Message Code field.</li> <li>Range—The message code must be within the range of codes specified by the Min. Message Code field and the Max. Message Code field.</li> </ul> |
| Message Code            | This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Message Code Operator field.<br>Enter the ICMP message code for this service object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Min. Message Code       | This field appears if you select Range in the Message Code Operator field.<br>Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Max. Message Code field.                                                                                                                                                                                                                                                                                                                                         |
| Max. Message Code       | This field appears if you select Range in the Message Code Operator field.<br>Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be greater than the number entered in the Min. Message Code field.                                                                                                                                                                                                                                                                                                                                         |



Table 4-17 Extended ACL Configuration Options (continued)

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Source Network           | <p>Defines the network traffic being received from the source network to the ACE:</p> <ul style="list-style-type: none"> <li>Any—Select the Any radio button to indicate that network traffic from any source is allowed.</li> <li>IP/Netmask—(IPv4 address type) Use this field to limit access to a specific source IP address. Enter the source IPv4 address that is allowed for this ACL and select its subnet mask.</li> <li>IP/Prefix-length—(IPv6 address type) Use this field to limit access to a specific source IP address. Enter the source IPv6 address that is allowed for this ACL and its prefix length.</li> <li>Network Object Group—Select a source network object group to apply to this ACL.</li> </ul>                            |
| Source Port Operator     | <p>This field appears if you select TCP or UDP in the Protocol field.</p> <p>Choose the operand to use to compare source port numbers:</p> <ul style="list-style-type: none"> <li>Equal To—The source port must be the same as the number in the Source Port Number field.</li> <li>Greater Than—The source port must be greater than the number in the Source Port Number field.</li> <li>Less Than—The source port must be less than the number in the Source Port Number field.</li> <li>Not Equal To—The source port must not equal the number in the Source Port Number field.</li> <li>Range—The source port must be within the range of ports specified by the Lower Source Port Number field and the Upper Source Port Number field.</li> </ul> |
| Source Port Number       | <p>This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Source Port Operator field.</p> <p>Enter the port name or number from which you want to permit or deny access.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Lower Source Port Number | <p>This field appears if you select Range in the Source Port Operator field.</p> <p>Enter the number of the lowest port from which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be less than the number entered in the Upper Source Port Number field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Upper Source Port Number | <p>This field appears if you select Range in the Source Port Operator field.</p> <p>Enter the port number of the upper port from which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Source Port Number field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 4-17 Extended ACL Configuration Options (continued)

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Destination</b>            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Destination Network           | <p>Defines the network traffic being transmitted to the destination network from the ACE:</p> <ul style="list-style-type: none"> <li>Any—Select the Any radio button to indicate that network traffic to any destination is allowed.</li> <li>IP/Netmask—(IPv4 address type) Use this field to limit access to a specific destination IP address. Enter the destination IPv4 address that is allowed for this ACL and select its subnet mask.</li> <li>IP/Prefix-length—(IPv6 address type) Use this field to limit access to a specific destination IP address. Enter the destination IPv6 address that is allowed for this ACL and its prefix length.</li> <li>Network Object Group—Select a destination network object group to apply to this ACL.</li> </ul>                                                    |
| Destination Port Operator     | <p>This field appears if you select TCP or UDP in the Protocol field.</p> <p>Select the operand to use to compare destination port numbers:</p> <ul style="list-style-type: none"> <li>Equal To—The destination port must be the same as the number in the Destination Port Number field.</li> <li>Greater Than—The destination port must be greater than the number in the Destination Port Number field.</li> <li>Less Than—The destination port must be less than the number in the Destination Port Number field.</li> <li>Not Equal To—The destination port must not equal the number in the Destination Port Number field.</li> <li>Range—The destination port must be within the range of ports specified by the Lower Destination Port Number field and the Upper Destination Port Number field.</li> </ul> |
| Destination Port Number       | <p>This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Destination Port Operator field.</p> <p>Enter the port name or number from which you want to permit or deny access.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Lower Destination Port Number | <p>This field appears if you select Range in the Destination Port Operator field.</p> <p>Enter the number of the lowest port to which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be less than the number entered in the Upper Destination Port Number field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Upper Destination Port Number | <p>This field appears if you select Range in the Destination Port Operator field.</p> <p>Enter the port number of the upper port to which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port Number field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 4-18 Protocol Names and Numbers

| Protocol Name <sup>1</sup> | Protocol Number | Description           |
|----------------------------|-----------------|-----------------------|
| AH                         | 51              | Authentication Header |
| EIGRP                      | 88              | Enhanced IGRP         |

**Table 4-18** Protocol Names and Numbers (continued)

| Protocol Name <sup>1</sup> | Protocol Number | Description                                 |
|----------------------------|-----------------|---------------------------------------------|
| ESP                        | 50              | Encapsulated Security Payload               |
| GRE                        | 47              | Generic Routing Encapsulation               |
| ICMP                       | 1               | Internet Control Message Protocol version 4 |
| ICMPv6 <sup>2</sup>        | 58              | Internet Control Message Protocol version 6 |
| IGMP                       | 2               | Internet Group Management Protocol          |
| IP                         | 0 (Any)         | Internet Protocol                           |
| IP-In-IP                   | 4               | IP-in-IP Layer 3 Tunneling Protocol         |
| OSPF                       | 89              | Open Shortest Path First                    |
| PIM                        | 103             | Protocol Independent Multicast              |
| TCP                        | 6               | Transmission Control Protocol               |
| UDP                        | 17              | User Datagram Protocol                      |

1. For a complete list of all protocols and their numbers, see the Internet Assigned Numbers Authority available at [www.iana.org/numbers/](http://www.iana.org/numbers/).
2. ICMPv6 is not available for an IPv4 service object group.

**Table 4-19** ICMP Type Names and Numbers

| ICMP Type Name       | Number |
|----------------------|--------|
| Alternate-Address    | 6      |
| Conversion-Error     | 31     |
| Echo                 | 8      |
| Echo-Reply           | 0      |
| Information-Reply    | 16     |
| Information-Request  | 15     |
| Mask-Reply           | 18     |
| Mask-Request         | 17     |
| Mobile-Redirect      | 32     |
| Parameter-Problem    | 12     |
| Redirect             | 5      |
| Router-Advertisement | 9      |
| Router-Solicitation  | 10     |
| Source-Quench        | 4      |
| Time-Exceeded        | 11     |
| Timestamp-Reply      | 14     |
| Timestamp-Request    | 13     |
| Traceroute           | 30     |
| Unreachable          | 3      |

**Table 4-20** *ICMPv6 Type Names and Numbers*

| ICMP Type Name      | Number |
|---------------------|--------|
| Echo                | 128    |
| Echo-Reply          | 129    |
| Information-Reply   | 140    |
| Information-Request | 139    |
| Parameter-Problem   | 4      |
| Redirect            | 137    |
| Time-Exceeded       | 3      |
| Traceroute          | 30     |
| Unreachable         | 1      |

- Step 5** Click **Add To Table** if you want to add one or more ACL entries to the table.  
See Step 4 for information on configuring the extended ACL entries.
- Step 6** Associate any VLAN interface to this ACL if required and do one of the following:
- Click **Deploy** to immediately deploy this configuration.
  - Click **Cancel** to exit without saving your entries and to return to the ACL Summary table.

**Related Topics**

- [Configuring Security with ACLs, page 4-58](#)
- [Creating ACLs, page 4-59](#)
- [Setting EtherType ACL Attributes, page 4-67](#)
- [Resequencing Extended ACLs, page 4-66](#)
- [Editing or Deleting ACLs, page 4-69](#)

## Resequencing Extended ACLs

Use this procedure to change the sequence of entries in an Extended ACL. EtherType ACL entries cannot be resequenced.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > context > Security > ACLs**.  
The ACLs table appears, listing the existing ACLs.
- Step 2** Choose the Extended ACL you want to renumber and then click the **Resequence** icon appearing to the left of the filter field.  
The ACL Line Number Resequence window appears.
- Step 3** In the Start field, enter the number that is to be assigned to the first entry in the ACL.

Valid entries are 1 to 2147483647.

- Step 4** In the Increment field, enter the number that is to be added to each entry in the ACL after the first entry. You can enter any integer.

Valid entries are 1 to 2147483647.

- Step 5** Do one of the following:

- Click **Resequenece** to save your entries and to return to the ACLs table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the ACLs table.

#### Related Topics

- [Configuring Security with ACLs, page 4-58](#)
- [Creating ACLs, page 4-59](#)
- [Setting EtherType ACL Attributes, page 4-67](#)
- [Setting Extended ACL Attributes, page 4-61](#)
- [Editing or Deleting ACLs, page 4-69](#)

## Setting EtherType ACL Attributes



#### Note

By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

You can configure an ACL that controls traffic based on its EtherType. An EtherType is a sub-protocol identifier. EtherType ACLs support Ethernet V2 frames. EtherType ACLs do not support 802.3-formatted frames because they use a length field as opposed to a type field. The only exception is bridge protocol data units (BPDUs), which are SNAP-encapsulated, and the ACE is designed to specifically handle BPDUs.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Security > ACLs**.
- The ACLs table appears, listing the existing ACLs.
- Step 2** Click **Add**.
- The New Access List configuration screen appears.
- Step 3** Enter the ACL name in the ACL Properties pane and choose Ethertype.
- Note that the only selectable IP Address Type is IPv4.
- Step 4** Choose one of the following radio buttons:
- **Deny** to indicate that the ACE is to block connections.
  - **Permit** to indicate that the ACE is to allow connections.
- Step 5** Choose one of the following from the Protocol field drop down menu for this ACL:
- **Any**—Specifies any EtherType.

- **BPDUs**—Specifies Bridge Protocol Data Units. The ACE receives trunk port (Cisco proprietary) BPDUs because ACE ports are trunk ports. Trunk BPDUs have VLAN information inside the payload, so the ACE modifies the payload with the outgoing VLAN if you allow BPDUs. If you configure redundancy, you must allow BPDUs on both interfaces with an EtherType ACL to avoid bridging loops. For information about configuring redundancy, see the [“Configuring High Availability” section on page 11-1](#).
- **IPv6**—Specifies Internet Protocol version 6.
- **MPLS**—Specifies Multi Protocol Label Switching. The MPLS selection applies to both MPLS unicast and MPLS multicast traffic. If you allow MPLS, ensure that Label Distribution Protocol (LDP) and Tag Distribution Protocol (TDP) TCP connections are established through the ACE by configuring both MPLS routers connected to the ACE to use the IP address on the ACE interface as the router-id for LDP or TDP sessions. LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.

**Step 6** Click **Add To Table** and add one or more ACL entries if required repeating [Step 4](#) and [Step 5](#) as needed.

**Step 7** Associate any VLAN interface to this ACL if required and do one of the following:

- Click **Deploy** to immediately deploy this configuration.
- Click **Cancel** to exit without saving your entries and to return to the ACL Summary table.

#### Related Topics

- [Configuring Security with ACLs, page 4-58](#)
- [Creating ACLs, page 4-59](#)
- [Setting Extended ACL Attributes, page 4-61](#)
- [Resequencing Extended ACLs, page 4-66](#)
- [Editing or Deleting ACLs, page 4-69](#)

## Viewing All ACLs by Context

Use this procedure to view all access control lists that have been configured.

#### Procedure

**Step 1** Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

**Step 2** Choose the virtual context with the ACLs you want to view, and then select **Security > ACLs**.

The ACLs table appears, listing the existing ACLs with their name, their type (Extended or EtherType), and any comments.

#### Related Topics

- [Configuring Virtual Context Expert Options, page 4-79](#)
- [Creating ACLs, page 4-59](#)
- [Setting EtherType ACL Attributes, page 4-67](#)

- [Setting Extended ACL Attributes, page 4-61](#)
- [Editing or Deleting ACLs, page 4-69](#)

## Editing or Deleting ACLs

Use this procedure to delete or edit an ACL or any of its subentries.

### Considerations

- You cannot mix IPv6 and IPv4 access-list entries in the same ACL.
- Before you change the IP address type for an existing ACL, you must remove the entries that are not applicable to the new IP address type.
- If you change the ACL protocol, the ACE removes all of the existing settings for the ACL.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Security > ACLs**.
- The ACLs table appears, listing the existing ACLs.
- Step 2** Click the radio button to the left of the ACL that you want to edit or delete.
- Expand entries if necessary by clicking the plus sign to the left of any ACL entry until you see the subentry ACL for which you are looking, or click the **Expand All** icon to view all ACLs and subentries.
- To hide the subentries under an ACL, click the minus sign to the left of any ACL entry. Click the **Collapse All** icon to hide the subentries under all ACLs.
- Step 3** Do one of the following:
- Click **Edit** if you are editing an ACL or one of its entries. Edit the entry using the summary information listed in [Table 4-16](#) if needed, and click **Deploy** when done.
  - Click **Delete** if you are deleting an ACL or one of its entries. A window appears asking you to confirm the deletion. If you click **OK**, the ACLs table refreshes without the deleted ACL.
- 

### Related Topics

- [Creating ACLs, page 4-59](#)
- [Setting EtherType ACL Attributes, page 4-67](#)
- [Setting Extended ACL Attributes, page 4-61](#)
- [Resequencing Extended ACLs, page 4-66](#)

## Displaying ACL Information and Statistics

You can display information and statistics for a particular ACL by using the **Details** button.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Security > ACLs**.

The ACLs table appears listing the existing ACLs.

- Step 2** In the ACLs table, choose an ACL, and click **Details**.

The **show access-list access-list detail** CLI command output appears. For details about the displayed output fields, see the *Security Guide, Cisco ACE Application Control Engine*, Chapter 1, Configuring Security Access Control Lists.

- Step 3** Click **Update Details** to refresh the output for the **show access-list access-list detail** CLI command.

- Step 4** Click **Close** to return to the ACLs table.

#### Related Topics

- [Configuring Virtual Context Expert Options, page 4-79](#)
- [Creating ACLs, page 4-59](#)
- [Setting Extended ACL Attributes, page 4-61](#)
- [Resequencing Extended ACLs, page 4-66](#)
- [Editing or Deleting ACLs, page 4-69](#)

## Configuring Object Groups

An **object group** is a logical grouping of objects such as hosts (servers and clients), services, and networks. When you create an object group, you select a type, such as network or service, and then specify the objects that belong to the groups. In all, there are four types of object groups: Network, protocol, service, and ICMP-type.

After you configure an object group, you can include it in ACLs, thereby including all objects within that group and reducing overall configuration size.

Use this procedure to configure object groups that you can associate with ACLs.

#### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

- Step 2** Click **Add** to create a new object group, or select an existing object group, and then click **Edit** to modify it.

The Object Groups configuration screen appears.

- Step 3** In the Name field, enter a unique name for this object group.

Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

- Step 4** In the Description field, enter a brief description for the object group.

- Step 5** In the Type field, select the type of object group you are creating:

- **Network**—The object group is based on a group of hosts or subnet IP addresses.
- **Service**—The object group is based on TCP or UDP protocols and ports, or ICMP types, such as echo or echo-reply.

- Step 6** Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts. The screen refreshes with tables additional configuration options.



- Click **Cancel** to exit without saving your entries and to return to the Object Groups table.
- Click **Next** to deploy your entries and to add another entry to the Object Groups table.

**Step 7** Configure objects for the object group.

For network-type object groups, options include:

- [Configuring IP Addresses for Object Groups, page 4-71](#)
- [Configuring Subnet Objects for Object Groups, page 4-72](#)

For service-type object groups, options include:

- [Configuring Protocols for Object Groups, page 4-73](#)
  - [Configuring TCP/UDP Service Parameters for Object Groups, page 4-73](#)
  - [Configuring ICMP Service Parameters for an Object Group, page 4-76](#)
- 

#### Related Topics

- [Configuring Virtual Context Expert Options, page 4-79](#)
- [Creating ACLs, page 4-59](#)
- [Setting Extended ACL Attributes, page 4-61](#)
- [Resequencing Extended ACLs, page 4-66](#)

## Configuring IP Addresses for Object Groups

Use this procedure to specify host IP addresses for network-type object groups.

#### Procedure

---

**Step 1** Choose **Config > Virtual Contexts > context > Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

**Step 2** Choose the object group you want to configure host IP addresses for and then click the **Host Setting For Object Group** tab.

The Host Setting For Object Group table appears.

**Step 3** Click **Add** to add an entry to this table.

**Step 4** Choose one of the following:

- **IPv4**—A host with an IPv4 IP address. In the IPv4 Address field, enter the IP address of a host to include in this group.
- **IPv6**—A host with an IPv6 IP address. In the IPv6 Address field, enter the IP address of a host to include in this group.

**Step 5** Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.

- Click **Next** to deploy your entries and to add another entry to the Host Setting table.
- 

#### Related Topics

- [Configuring Object Groups, page 4-70](#)
- [Configuring Subnet Objects for Object Groups, page 4-72](#)
- [Configuring Protocols for Object Groups, page 4-73](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 4-73](#)
- [Configuring ICMP Service Parameters for an Object Group, page 4-76](#)

## Configuring Subnet Objects for Object Groups

Use this procedure to specify subnet objects for a network-type object group.

#### Procedure

---

- Step 1** Choose **Config > Virtual Contexts > context > Security > Object Groups**.  
The Object Groups table appears, listing existing object groups.
- Step 2** Choose the object group you want to configure subnet objects for and then click the **Network Setting For Object Group** tab.  
The Network Setting For Object Group table appears.
- Step 3** Click **Add** to add an entry to this table.
- Step 4** Choose one of the following:
- **IPv4**—A subnet object with an IPv4 IP address. In the IPv4 Address field, enter the IP address. In the Netmask field, select the subnet mask for this subnet object.
  - **IPv6**—A object with an IPv6 IP address. In the IPv6 Address field, enter the IP address. In the Network Prefix Length field, enter the prefix length for this object.
- Step 5** Do one of the following:
- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
  - Click **Cancel** to exit this procedure without saving your entries.
  - Click **Next** to deploy your entries and to add another entry to the Network Setting table.
- 

#### Related Topics

- [Configuring Object Groups, page 4-70](#)
- [Configuring IP Addresses for Object Groups, page 4-71](#)
- [Configuring Protocols for Object Groups, page 4-73](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 4-73](#)
- [Configuring ICMP Service Parameters for an Object Group, page 4-76](#)

## Configuring Protocols for Object Groups

Use this procedure to specify protocols for a service-type object group.

### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; <i>context</i> &gt; Security &gt; Object Groups</b> .<br>The Object Groups table appears, listing existing object groups.                                                                                                                                                                                                                 |
| <b>Step 2</b> | Choose an existing service-type object group and then click the <b>Protocol Selection</b> tab.<br>The Protocol Selection table appears.                                                                                                                                                                                                                                               |
| <b>Step 3</b> | Click <b>Add</b> to add an entry to this table.                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 4</b> | In the Protocol Number field, select the protocol or protocol number to add to this object group.<br>See <a href="#">Table 4-18</a> for common protocols and their numbers.                                                                                                                                                                                                           |
| <b>Step 5</b> | Do one of the following: <ul style="list-style-type: none"><li>• Click <b>Deploy Now</b> to immediately deploy this configuration. This option appears for virtual contexts.</li><li>• Click <b>Cancel</b> to exit this procedure without saving your entries.</li><li>• Click <b>Next</b> to deploy your entries and to add another entry to the Protocol Selection table.</li></ul> |
- 

### Related Topics

- [Configuring Object Groups, page 4-70](#)
- [Configuring IP Addresses for Object Groups, page 4-71](#)
- [Configuring Subnet Objects for Object Groups, page 4-72](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 4-73](#)
- [Configuring ICMP Service Parameters for an Object Group, page 4-76](#)

## Configuring TCP/UDP Service Parameters for Object Groups

Use this procedure to add TCP or UDP service objects to a service-type object group.

### Procedure

- 
- |               |                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; <i>context</i> &gt; Security &gt; Object Groups</b> .<br>The Object Groups table appears, listing existing object groups. |
| <b>Step 2</b> | Choose an existing service-type object group and then select the TCP/UDP Service Parameters tab.<br>The TCP/UDP Service Parameters table appears.                     |
| <b>Step 3</b> | Click <b>Add</b> to add an entry to this table.                                                                                                                       |
| <b>Step 4</b> | Configure TCP or UDP service objects using the information in <a href="#">Table 4-21</a> .                                                                            |

Table 4-21 TCP and UDP Service Parameters

| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol                  | <p>Select the protocol for this service object:</p> <ul style="list-style-type: none"> <li>TCP—TCP is the protocol for this service object.</li> <li>UDP—UDP is the protocol for this service object.</li> <li>TCP And UDP—Both TCP and UDP are the protocols for this service object.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| Source Port Operator      | <p>Select the operand to use when comparing source port numbers for this service object:</p> <ul style="list-style-type: none"> <li>Equal To—The source port must be the same as the number in the Source Port field.</li> <li>Greater Than—The source port must be greater than the number in the Source Port field.</li> <li>Less Than—The source port must be less than the number in the Source Port field.</li> <li>Not Equal To—The source port must not equal the number in the Source Port field.</li> <li>Range—The source port must be within the range of ports specified by the Lower Source Port field and the Upper Source Port field.</li> </ul>                                     |
| Source Port               | <p>This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Source Port Operator field.</p> <p>Enter the source port name or number for this service object.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Lower Source Port         | <p>This field appears if you select Range in the Source Port Operator field.</p> <p>Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the Upper Source Port field.</p>                                                                                                                                                                                                                                                                                                                                                                     |
| Upper Source Port         | <p>This field appears if you select Range in the Source Port Operator field.</p> <p>Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 2 to 65535. The number in this field must be greater than the number entered in the Lower Source Port field.</p>                                                                                                                                                                                                                                                                                                                                                                     |
| Destination Port Operator | <p>Choose the operand to use when comparing destination port numbers:</p> <ul style="list-style-type: none"> <li>Equal To—The destination port must be the same as the number in the Destination Port field.</li> <li>Greater Than—The destination port must be greater than the number in the Destination Port field.</li> <li>Less Than—The destination port must be less than the number in the Destination Port field.</li> <li>Not Equal To—The destination port must not equal the number in the Destination Port field.</li> <li>Range—The destination port must be within the range of ports specified by the Lower Destination Port field and the Upper Destination Port field.</li> </ul> |
| Destination Port          | <p>This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Destination Port Operator field.</p> <p>Enter the destination port name or number for this service object.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Table 4-21 TCP and UDP Service Parameters (continued)

| Field                  | Description                                                                                                                                                                                                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lower Destination Port | This field appears if you select <i>Range</i> in the Destination Port Operator field.<br><br>Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 0 to 65535. The number in this field must be less than the number entered in the Upper Destination Port field. |
| Upper Destination Port | This field appears if you select <i>Range</i> in the Destination Port Operator field.<br><br>Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port field. |

**Step 5** Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the TCP/UDP Service Parameters table.

**Related Topics**

- [Configuring Object Groups, page 4-70](#)
- [Configuring IP Addresses for Object Groups, page 4-71](#)
- [Configuring Subnet Objects for Object Groups, page 4-72](#)
- [Configuring Protocols for Object Groups, page 4-73](#)
- [Configuring ICMP Service Parameters for an Object Group, page 4-76](#)

## Configuring ICMP Service Parameters for an Object Group

Use this procedure to add ICMP service parameters to a service-type object group.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Security > Object Groups**.  
The Object Groups table appears, listing existing object groups.
- Step 2** Choose an existing service-type object group and then click the **ICMP Service Parameters** tab.  
The ICMP Service Parameters table appears.
- Step 3** Click **Add** to add an entry to this table.
- Step 4** Configure ICMP type objects using the information in [Table 4-22](#).

**Table 4-22** ICMP Type Service Parameters

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICMP Version          | Check either of the following check boxes for the ICMP version: <ul style="list-style-type: none"> <li>ICMP—Internet Control Message Protocol (ICMP) for Internet Protocol version 4 (IPv4).</li> <li>ICMPv6—Internet Control Message Protocol version 6 (ICMPv6) for Internet Protocol version 6 (IPv6).</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| ICMP Type             | Select the ICMP type or number for this service object. <a href="#">Table 4-23</a> lists common ICMP types and numbers. <a href="#">Table 4-24</a> lists the ICMPv6 types and numbers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Message Code Operator | Select the operand to use when comparing message codes for this service object: <ul style="list-style-type: none"> <li>Equal To—The message code must be the same as the number in the Message Code field.</li> <li>Greater Than—The message code must be greater than the number in the Message Code field.</li> <li>Less Than—The message code must be less than the number in the Message Code field.</li> <li>Not Equal To—The message code must not equal the number in the Message Code field.</li> <li>Range—The message code must be within the range of codes specified by the Min. Message Code field and the Max. Message Code field.</li> </ul> |
| Message Code          | This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Message Code Operator field.<br>Enter the ICMP message code for this service object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 4-22** *ICMP Type Service Parameters (continued)*

| Field             | Description                                                                                                                                                                                                                                                                                                         |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Min. Message Code | This field appears if you select Range in the Message Code Operator field.<br>Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Max. Message Code field. |
| Max. Message Code | This field appears if you select Range in the Message Code Operator field.<br>Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be greater than the number entered in the Min. Message Code field. |

**Table 4-23** *ICMP Type Numbers and Names*

| ICMP Type Name       | Number |
|----------------------|--------|
| Alternate-Address    | 6      |
| Conversion-Error     | 31     |
| Echo                 | 8      |
| Echo-Reply           | 0      |
| Information-Reply    | 16     |
| Information-Request  | 15     |
| Mask-Reply           | 18     |
| Mask-Request         | 17     |
| Mobile-Redirect      | 32     |
| Parameter-Problem    | 12     |
| Redirect             | 5      |
| Router-Advertisement | 9      |
| Router-Solicitation  | 10     |
| Source-Quench        | 4      |
| Time-Exceeded        | 11     |
| Timestamp-Reply      | 14     |
| Timestamp-Request    | 13     |
| Traceroute           | 30     |
| Unreachable          | 3      |

**Table 4-24** *ICMPv6 Type Names and Numbers*

| ICMP Type Name | Number |
|----------------|--------|
| Echo           | 128    |
| Echo-Reply     | 129    |

*Table 4-24 ICMPv6 Type Names and Numbers (continued)*

| ICMP Type Name      | Number |
|---------------------|--------|
| Information-Reply   | 140    |
| Information-Request | 139    |
| Parameter-Problem   | 4      |
| Redirect            | 137    |
| Time-Exceeded       | 3      |
| Traceroute          | 30     |
| Unreachable         | 1      |

**Step 5** Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the ICMP Service Parameters table.

#### Related Topics

- [Configuring Object Groups, page 4-70](#)
- [Configuring IP Addresses for Object Groups, page 4-71](#)
- [Configuring Subnet Objects for Object Groups, page 4-72](#)
- [Configuring Protocols for Object Groups, page 4-73](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 4-73](#)



# Configuring Virtual Context Expert Options

Table 4-25 identifies ACE Appliance Device Manager virtual context Expert configuration options and related topics for more information.

**Table 4-25** *Virtual Context Expert Configuration Options*

| Expert Configuration Options                                                                                                    | Related Topics                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establish traffic policies by classifying types of network traffic and then applying rules and actions for handling the traffic | <ul style="list-style-type: none"><li>• <a href="#">Configuring Traffic Policies, page 12-1</a></li><li>• <a href="#">Configuring Virtual Context Class Maps, page 12-8</a></li><li>• <a href="#">Configuring Virtual Context Policy Maps, page 12-34</a></li></ul> |
| Configure HTTP header modify action lists                                                                                       | <a href="#">Configuring an HTTP Header Modify Action List, page 12-90</a>                                                                                                                                                                                           |
| Configure HTTP optimization action lists                                                                                        | <a href="#">Configuring an HTTP Optimization Action List, page 13-3</a>                                                                                                                                                                                             |

## Managing Virtual Contexts

You can perform the following administrative actions on virtual contexts:

- [Synchronizing Virtual Context Configurations, page 4-79](#)
- [Editing Virtual Contexts, page 4-84](#)
- [Deleting Virtual Contexts, page 4-84](#)
- [Viewing All Virtual Contexts, page 4-84](#)

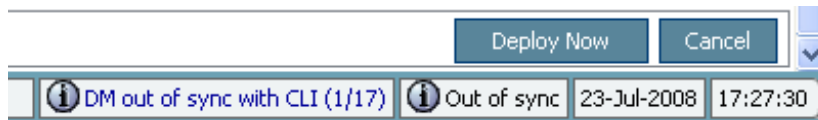
## Synchronizing Virtual Context Configurations

ACE Appliance Device Manager identifies virtual contexts with different configurations on the ACE appliance and in ACE Appliance Device Manager. Discrepancies between these configurations occur when a user configures the ACE appliance directly using the CLI instead of the ACE Appliance Device Manager.

The ACE Appliance Device Manager automatically polls the CLI once every two minutes. When you use the CLI to change a virtual context's configuration on the ACE appliance, and the Device Manager detects an out-of-band configuration change in a context during this polling period, the configuration changes are applied by the Device Manager.

The status bar at the bottom right of the ACE Appliance Device Manager displays two indicators for you to monitor CLI and DM GUI synchronization status (Figure 4-1). One indicator displays ACE appliance Device Manager GUI and CLI synchronization status along with a summary count of the contexts in the various synchronization states, and the other indicator displays CLI synchronization and polling status for the active context. The status bar auto-refreshes every 10 seconds.

**Figure 4-1** CLI and DM GUI Synchronization Status Bar



For example, as illustrated in Figure 4-1, the message “DM out of sync with CLI (1/17)” indicates that out of the 17 configured contexts, one context is in the “Out of sync” CLI synchronization status state.



#### Note

If a user attempt to deploy a configuration from the ACE Appliance Device Manager (clicks the Deploy Now button) while synchronization is in process for a particular context, an error message appears indicating that synchronization is in process and the user should try to deploy the configuration at a later point in time.

ACE Appliance Device Manager provides the following options for identifying and synchronizing configuration discrepancies:

- [Viewing Virtual Context Synchronization Status](#), page 4-80
- [High Availability and Virtual Context Configuration Status](#), page 4-81
- [Manually Synchronizing Individual Virtual Context Configurations](#), page 4-82
- [Manually Synchronizing All Virtual Context Configurations](#), page 4-83

## Viewing Virtual Context Synchronization Status

ACE Appliance Device Manager identifies virtual contexts with different configurations in the ACE appliance and in the ACE Appliance Device Manager. Discrepancies between these configurations occur when a user configures the ACE appliance directly using the CLI instead of ACE Appliance Device Manager.

In Config screens, CLI and DM GUI configuration status appears in the following locations in the ACE Appliance Device Manager:

- In the All Virtual Contexts table (**Config > Virtual Contexts**), in the CLI Sync Status column.
- The status bar at the bottom of the ACE Appliance Device Manager browser (see Figure 4-1).

The following reported CLI synchronization states appear in the All Virtual Context table:

- OK—The configurations for the selected virtual context are synchronized with the CLI.
- Out Of Sync—The configurations for the selected virtual context are not synchronized with the CLI.
- Sync In Progress—The CLI to DM GUI synchronization for this context is in process, either started automatically by the ACE Appliance Device Manager or manually (using either the CLI Sync or CLI Sync All buttons).

- **Sync Failed**—The last synchronization attempt failed and you must perform a manual synchronization using either the CLI Sync or CLI Sync All buttons. The failed state could be due to an unrecognized CLI command on the context, or due to an internal error on the ACE Appliance Device Manager. Once the problem is resolved, another manual synchronization will be required to move the context into the OK synchronization state.

The status bar at the bottom of the ACE Appliance Device Manager browser (see [Figure 4-1](#)) displays DM GUI and CLI synchronization status along with a summary count of the contexts in the various synchronization states. For example, the message “DM out of sync with CLI (1/10), DM sync with CLI failed (2/10)” indicates that out of the 10 configured contexts, one context is in the “Out Of Sync” state and two are in the “Sync Failed” state, and the remaining contexts are in the “OK” state. The status bar auto-refreshes every 10 seconds.

**Note**

Clicking the summary count in the status bar from any context-specific page accesses the All Virtual Contexts table. You can view the CLI synchronization status for all contexts.

If a user changes the configuration for a context by using the CLI while you are viewing the All Virtual Contexts table, the information in the CLI Sync Status column does not automatically update to reflect an out-of-sync state. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view out-of-sync configurations.

For information on synchronizing out-of-sync virtual context configurations, see the following topics:

- [Manually Synchronizing Individual Virtual Context Configurations, page 4-82](#)
- [Manually Synchronizing All Virtual Context Configurations, page 4-83](#)

**Related Topics**

- [Synchronizing Virtual Context Configurations, page 4-79](#)
- [High Availability and Virtual Context Configuration Status, page 4-81](#)

## High Availability and Virtual Context Configuration Status

In a high availability pair, the two configured virtual contexts synchronize with each other as part of their ongoing communications. However, their copies do not synchronize in ACE Appliance Device Manager and the configuration on the standby member can become out of sync with the configuration on the ACE appliance.

After the active member of a high availability pair fails and the standby member becomes active, ACE Appliance Device Manager on the newly active member detects any out-of-sync virtual context configurations and reports that status in the All Virtual Contexts table so that you can synchronize the virtual context configurations.

**Note**

When a virtual context is in either the Standby Hot or Standby Warm state (see the [“High Availability Polling” section on page 11-2](#)), the virtual context may receive configuration changes from its ACE peer without updating the Device Manager GUI. As a result, the ACE appliance Device Manager GUI will be out of synchronization with the CLI configuration. If you need to check configuration on a standby virtual context using HA Tracking And Failure Detection (see the [“Tracking VLAN Interfaces for High Availability” section on page 11-19](#)), we recommend that you first perform a manual synchronization using either the CLI Sync or CLI Sync All buttons before checking the configuration values.

For information on synchronizing out-of-sync virtual context configurations, see the following topics:

- [Manually Synchronizing Individual Virtual Context Configurations, page 4-82](#)
- [Manually Synchronizing All Virtual Context Configurations, page 4-83](#)

#### Related Topics

- [Viewing Virtual Context Synchronization Status, page 4-80](#)
- [Configuring ACE High Availability, page 11-8](#)

## Manually Synchronizing Individual Virtual Context Configurations

Use this procedure if you want to manually synchronize the configuration for a selected virtual context. This procedure removes the configuration information for this virtual context from ACE Appliance Device Manager and replaces it with its CLI configuration from the ACE appliance. You may want to manually synchronize a virtual context configuration if you do not want to wait for auto synchronization to occur and you want the CLI context configuration changes immediately applied to the ACE Appliance Device Manager.

#### Procedure

---

**Step 1** Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears. Contexts with configurations that are not synchronized display *Out of sync* in the CLI Sync Status column.



**Note** If a user changes the configuration for a context by using the CLI while you are viewing the All Virtual Contexts table, the information in the CLI Sync Status column is not automatically updated to reflect an out-of-sync state. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view out-of-sync configurations.

---

**Step 2** Choose the virtual context with the configuration that you want to synchronize and then click **CLI Sync**. A window appears, asking you to confirm the operation.

**Step 3** Click **OK** to upload the configuration from the ACE appliance or **Cancel** to exit this procedure without uploading the configuration.

If you click **OK**, the screen reports progress and then refreshes with updated configuration status in the CLI Sync Status column.

---

#### Related Topics

- [Synchronizing Virtual Context Configurations, page 4-79](#)
- [Viewing Virtual Context Synchronization Status, page 4-80](#)
- [Manually Synchronizing All Virtual Context Configurations, page 4-83](#)

## Manually Synchronizing All Virtual Context Configurations

Use this procedure to manually synchronize all virtual context configurations. This procedure removes all virtual context configurations from ACE Appliance Device Manager and replaces them with their CLI configurations from the ACE appliance. You may want to manually synchronize all virtual contexts if you do not want to wait for auto-synchronization to occur and you want the CLI context configuration changes immediately applied to the ACE Appliance Device Manager.

This operation can take several minutes to finish, depending on the number of virtual contexts.



**Note**

If you configure a virtual server using the CLI and then use the CLI Sync All option (**Config > Virtual Contexts**) to manually synchronize configurations, the configuration that appears in ACE Appliance Device Manager for the virtual server might not display all configuration options for that virtual server. The configuration that appears in ACE Appliance Device Manager depends on a number of items, such as the protocols configured in class maps or the rules defined for policy maps.

For example, if you configure a virtual server on the CLI that includes a class map that can match any protocol, you will not see the virtual server Application Acceleration and Optimization configuration subset in ACE Appliance Device Manager.



**Note**

This procedure is available for only the admin user in an Admin context.

### Procedure

**Step 1** Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

**Step 2** Click **CLI Sync All**. A window appears, asking you to confirm the operation.

**Step 3** Click **OK** to continue with this option or click **Cancel** to exit this procedure.

If you click **OK**, the screen refreshes with the All Virtual Contexts table listing the contexts that have been imported so far and displays configuration update progress.



**Note**

Depending on the number of contexts, this process can take several minutes to complete.

**Step 4** Click **Refresh** to view additional contexts that have been imported.

### Related Topics

- [Synchronizing Virtual Context Configurations, page 4-79](#)
- [Manually Synchronizing Individual Virtual Context Configurations, page 4-82](#)

## Editing Virtual Contexts

Use this procedure to modify the configuration of an existing virtual context.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts**.  
The All Virtual Contexts table appears.
- Step 2** Choose the virtual context and then select the configuration attributes you want to modify.  
For information on configuration options, see the [“Configuring Virtual Contexts” section on page 4-7](#).
- Step 3** Click **Deploy Now** to deploy this configuration on the ACE appliance.  
To exit a procedure without saving your entries, click **Cancel**, or select another item in the menu bar or another attribute to configure. A window appears, confirming that you have not saved your entries.
- 

### Related Topic

- [Using Virtual Contexts, page 4-2](#)

## Deleting Virtual Contexts

Use this procedure to remove an existing virtual context.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts**.  
The All Virtual Contexts table appears.
- Step 2** Choose the virtual context you want to remove and then click **Delete**.  
A window appears, asking you to confirm the deletion.
- Step 3** Do one of the following:
- Click **OK** to delete the selected context. The device tree refreshes and the deleted context no longer appears.
  - Click **Cancel** to exit this procedure and to retain the selected context.
- 

### Related Topic

- [Using Virtual Contexts, page 4-2](#)

## Viewing All Virtual Contexts

To view all virtual contexts, choose **Config > Virtual Contexts**. The All Virtual Contexts table appears.

**Note**

Clicking the summary count in the status bar from any context-specific page accesses the All Virtual Contexts table. You can then review the synchronization configuration details for all of the available contexts. If you are not the administrator, you will only see the details for your user context.

The All Virtual Contexts table displays the following information for each virtual context

- Name
- Resource class
- Management IP address
- Virtual context synchronization status; that is, whether the ACE Appliance Device Manager GUI and CLI configurations for the context are synchronized, not synchronized, being synchronized, or the synchronization attempt failed. For more information, see the [“Viewing Virtual Context Synchronization Status” section on page 4-80](#).
- ACE high availability state; for more information on the available ACE high availability states, see the [“High Availability Polling” section on page 11-2](#).

**Note**

For information on the implication of ACE high availability on ACE appliance Device Manager GUI and CLI configuration synchronization, see the [“Synchronizing High Availability Configurations with ACE Appliance Device Manager” section on page 11-6](#).

- State of the ACE high availability peer
- ACE high availability peer name
- Whether automatic synchronization for high availability pairs has been configured

**Note**

If a user changes the configuration for a context by using the CLI while you are viewing the All Virtual Contexts table, or if the high availability state changes, the information in the table columns does not automatically update to reflect an out-of-sync state. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view out-of-sync configurations.

**Note**

If a user creates a new virtual context in a different session while you are viewing the All Virtual Contexts table, the new virtual context does not automatically appear in this table. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view newly-created contexts.

Polling status for the selected context appears above the content area in the upper right corner (see [Figure 1-2](#)). [Table 14-1](#) describes the various polling states.

From this screen you can:

- Add a new virtual context—See the [Creating Virtual Contexts, page 4-2](#).
- Edit an existing virtual context—See [Configuring Virtual Contexts, page 4-7](#).
- Delete an existing virtual context—See [Deleting Virtual Contexts, page 4-84](#).
- Manually synchronize ACE Appliance Device Manager and CLI configurations for one or all virtual contexts—See [Synchronizing Virtual Context Configurations, page 4-79](#).

**Related Topic**

- [Managing Virtual Contexts, page 4-79](#)





## CHAPTER 5

# Configuring Virtual Servers

---

This chapter provides an overview of server load balancing and procedures for configuring virtual servers for load balancing on an ACE appliance.



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

This chapter contains the following topics:

- [Load Balancing Overview, page 5-1](#)
- [Configuring Virtual Servers, page 5-2](#)
- [Managing Virtual Servers, page 5-63](#)

## Load Balancing Overview

Server load balancing (SLB) is the process of deciding to which server a load-balancing device should send a client request for service. For example, a client request can consist of an HTTP GET for a Web page or an FTP GET to download a file. The job of the load balancer is to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Depending on the load-balancing algorithm or predictor that you configure, the ACE appliance performs a series of checks and calculations to determine the server that can best service each client request. The ACE appliance bases server selection on several factors, including the server with the fewest connections with respect to load, source or destination address, cookies, URLs, or HTTP headers.

The ACE Appliance Device Manager allows you to configure load balancing as described in the following topics:

- Virtual servers—See [Configuring Virtual Servers, page 5-2](#).
- Real servers—See [Configuring Real Servers, page 6-5](#).
- Server farms—See [Configuring Server Farms, page 6-18](#).

- Sticky groups—See [Configuring Sticky Groups, page 7-11](#).
- Parameter maps—See [Configuring Parameter Maps, page 8-1](#).

For information about SLB as configured and performed by the ACE appliance, see the following topics:

- [Configuring Virtual Servers, page 5-2](#)
- [Load-Balancing Predictors, page 6-2](#)
- [Real Servers, page 6-3](#)
- [Server Farms, page 6-5](#)
- [Configuring Health Monitoring, page 6-39](#)
- [TCL Scripts, page 6-40](#)
- [Configuring Sticky Groups, page 7-11](#)

## Configuring Virtual Servers

In a load-balancing environment, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. A virtual server is bound to physical services running on real servers in a server farm and uses IP address and port information to distribute incoming client requests to the servers in the server farm according to a specified load-balancing algorithm.

You use class maps to configure a virtual server address and definition. The load-balancing predictor algorithms (for example, round-robin, least connections, and so on) determine the servers to which the ACE sends connection requests.

For more information about virtual servers and the ACE Appliance Device Manager, see the following topics:

- [Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 5-2](#)
- [Information About Using Device Manager to Configure Virtual Servers, page 5-5](#)
- [Virtual Server Configuration Procedure, page 5-7](#)

## Understanding Virtual Server Configuration and ACE Appliance Device Manager

The ACE Appliance Device Manager Virtual Server configuration interface, an abstraction of the Modular Policy CLI, simplifies, reorders, and makes more atomic the configuration and deployment of a functional load-balancing environment. With simplification or abstraction, some constraints or limitations are necessarily introduced. This section identifies the constraints and framework used by ACE Appliance Device Manager for virtual server configuration.

In ACE Appliance Device Manager, a viable virtual server has the following attributes:

- A single Layer 3/Layer 4 match condition  
This means that you can specify only a single IP address (or single IP address range if an IPv4 netmask or IPv6 prefix length is used), with only a single port (or port range). Having a single match condition greatly simplifies and aids virtual server configuration.
- A default Layer 7 action
- A Layer 7 policy map

- A Layer 3/Layer 4 class map
- A multi-match policy map, a class-map match, and an action

In addition:

- The virtual server multi-match policy map is associated with an interface or is global.
- The name of the virtual server is derived from the name of the Layer 3/Layer 4 class map.

[Example 5-1](#) shows the minimum configuration statements required for a virtual server.

**Example 5-1 Minimum Configuration Required for a Virtual Server**

**IPv4**

```
class-map match-all Example_VIP
 2 match virtual-address 10.10.10.10 tcp eq www
policy-map type loadbalance first-match Example_VIP-l7slb
 class class-default
 forward
policy-map multi-match int10
 class Example_VIP
 loadbalance policy Example_VIP-l7slb

interface vlan 10
 ip address 192.168.65.37 255.255.255.0
 service-policy input int10
 no shutdown
```

**IPv6**

```
class-map match-all Example2_VIP
 2 match virtual-address 2001:DB8:10::5 tcp eq www
policy-map type loadbalance first-match Example2_VIP-l7slb
 class class-default
 forward
policy-map multi-match int11
 class Example2_VIP
 loadbalance policy Example2_VIP-l7slb

interface vlan 10
 ip address 2001:DB8:10::21/64
 service-policy input int11
 no shutdown
```

Note the following items regarding the ACE Appliance Device Manager and virtual servers:

- Additional configuration options  
The Virtual Server configuration screen allows you to configure additional items for a functional VIP. These items include server farms, sticky groups, real servers, probes, parameter maps, inspection, class maps, and inline match conditions. Because too many items on a screen can be overwhelming, not all configuration options appear on Virtual Server configuration screen, such as sticky statics or backup real servers. These options are available elsewhere in the ACE Appliance Device Manager interface instead of on the Virtual Server configuration screen.

- Configuration options and roles

To support and maintain the separation of roles, some objects cannot be configured using the Virtual Server configuration screen. These objects include SSL certificates, SSL keys, NAT pools, interface IP addresses, and ACLs. Providing these options as separate configuration options in the ACE Appliance Device Manager interface ensures that a user who can view or modify virtual servers or aspects of virtual servers cannot create or delete virtual servers.

- RBAC role and domain requirements

If you want to create, modify, or delete a virtual server, we recommend that you use the pre-defined Admin role (see [Table 15-4](#)). Only the Admin pre-defined role supports the ability to successfully deploy a functional virtual server from the ACE appliance Device Manager.

If a user prefers to be assigned a custom role, and wants the ability to create, modify, or delete a virtual server, that user requires the proper role permissions to be defined by the administrator to allow them to perform those virtual server activities.


**Note**

A user must be assigned with a default domain (default-domain) to be able to configure a virtual server. A domain is the namespace in which a user operates.

Included below are a list of RBAC permissions which are required for a user to create, modify, or delete a virtual server:

| Rule | Type   | Permission | Feature     |
|------|--------|------------|-------------|
| 1.   | Permit | Create     | real        |
| 2.   | Permit | Create     | serverfarm  |
| 3.   | Permit | Create     | vip         |
| 4.   | Permit | Create     | probe       |
| 5.   | Permit | Create     | loadbalance |
| 6.   | Permit | Create     | nat         |
| 7.   | Permit | Create     | interface   |
| 8.   | Permit | Create     | connection  |
| 9.   | Permit | Create     | ssl         |
| 10.  | Permit | Create     | pki         |
| 11.  | Permit | Create     | sticky      |
| 12.  | Permit | Create     | inspect     |

Note that certain configured virtual servers may only cover a subset of the features and may not require all the permissions outlined above. In general, the above set of permissions are required for allowing users to configure all elements of a virtual server.

For background information, see the “[Managing User Roles](#)” section in [Chapter 15, “Managing the ACE Appliance”](#).

**Related Topics**

- [Configuring Virtual Servers, page 5-2](#)
- [Information About Using Device Manager to Configure Virtual Servers, page 5-5](#)
- [Virtual Server Configuration Procedure, page 5-7](#)

## Information About Using Device Manager to Configure Virtual Servers

It is important to understand the following when using the ACE Appliance Device Manager to configure virtual servers:

- **Virtual server configuration screens**

The ACE Appliance Device Manager Virtual Server configuration screens are designed to aid you in configuring virtual servers by presenting configuration options that are relevant to your choices. For example, the protocols that you select in the Properties configuration subset determine the other configuration subsets that appear.

- **Use the virtual server configuration method that suits you**

The ACE Appliance Device Manager Virtual Server configuration screens simplify the process of creating, modifying, and deploying virtual servers by displaying those options that you are most likely to use. In addition, as you specify attributes for a virtual server, such as protocols, the interface refreshes with related configuration options, such as Protocol Inspection or Application Acceleration and Optimization, thereby speeding virtual server configuration and deployment.

While Virtual Server configuration screens remove some configuration complexities, they have a few constraints that the Expert configuration options do not. If you are comfortable using the CLI, you can use the Expert options (such as **Config > Virtual Contexts > context > Expert > Class Maps or Policy** or **Config > Virtual Contexts > context > Load Balancing > Parameter Map** to configure more complex attributes of virtual servers, traffic policies, and parameter maps.

- **Synchronizing virtual server configurations**

When you use the CLI to change a virtual context's configuration on the ACE appliance, the ACE Appliance Device Manager periodically polls the CLI (approximately once every two minutes) for configuration changes. When it detects an out-of-band configuration change in a context, the changes are applied to the configuration maintained by ACE Appliance Device Manager. The status bar at the bottom of the ACE Appliance Device Manager indicates a summary count of the contexts in the various synchronization states

If you configure a virtual server using the CLI and then use the CLI Sync option (**Config > Virtual Contexts > CLI Sync**) to manually synchronize configurations, the configuration that appears in the ACE Appliance Device Manager for the virtual server might not display all configuration options for that virtual server. The configuration that appears in the ACE Appliance Device Manager depends on a number of items, such as the protocols configured in class maps or the rules defined for policy maps.

For example, if you configure a virtual server on the CLI that includes a class map that can match any protocol, you will not see the virtual server Application Acceleration and Optimization configuration subset in the ACE Appliance Device Manager.

- **Modifying shared objects**

Modifying an object that is used by multiple virtual servers, such as a server farm, real server, or parameter map, could impact the other virtual servers. See [Shared Objects and Virtual Servers, page 5-9](#) for more information about modifying objects used by multiple virtual servers.

### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 5-2](#)
- [Virtual Server Configuration Procedure, page 5-7](#)

## Virtual Server Usage Guidelines

The Virtual Server configuration window provides you with numerous configuration options. However, instead of setting every option in one pass, configure your virtual server in stages. The first stage should always be to establish basic “pass through” connectivity with simple load balancing and include minimal additional features. This level of setup should verify that ports, VLANs, interfaces, SSL termination (if applicable), and real servers have been set up properly, enabling basic connectivity.

After you establish this level of connectivity, additional virtual server features will be easier to configure and troubleshoot.

Common features to add to a working basic virtual server are as follows:

- Health monitoring probes
- Session persistence (sticky)
- Additional real servers to a server farm
- Application protocol inspection
- Application acceleration and optimization

[Table 5-1](#) identifies and describes virtual server configuration subsets with links to related topics for configuration information.

### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Information About Using Device Manager to Configure Virtual Servers, page 5-5](#)
- [Virtual Server Testing and Troubleshooting, page 5-6](#)
- [Virtual Server Configuration Procedure, page 5-7](#)

## Virtual Server Testing and Troubleshooting

As outlined in the “[Virtual Server Usage Guidelines](#)” [section on page 5-6](#), first set up a basic virtual server that only enables connectivity and simple load balancing, such as round-robin between two real servers. Next, use a client, such as a web browser, to send a request from the client network to the virtual server VIP address. If the request is successful, you can now make changes or add virtual server features.

If the request is not successful, begin virtual server troubleshooting as outlined in the following sequence:

1. Wait and retry your request after a minute or two, especially if the existing ACE configuration is large. It can take seconds or even minutes for configuration changes to affect how traffic is handled by ACE.
2. Click the **Details** button in the lower right of the Virtual Server page. The Details button displays the output of the **show service-policy** CLI command.
3. Verify that the VIP State in the **show service-policy** CLI command output is **INSERVICE**. If the VIP state is not **INSERVICE**, this may indicate the following:
  - The virtual server has been manually disabled in the configuration.
  - The real servers are all unreachable from ACE or manually disabled. If all of a virtual server's real servers are out of service due to one of those reasons, the virtual server itself will be marked Out Of Service.

4. Verify the Hit Count in the **show service-policy** CLI command output. Hit Count shows the number of requests received by ACE. This value should increase for each request attempted by your client. If the hit count does not increase with each request, this indicates that the request is not reaching your virtual server configuration.

This could be a problem with one of the following:

- A physical connection.
- VLAN or VLAN interface configuration.
- Missing or incorrect ACL applied to the client interface.
- Incorrect IP address (that is, a VIP that is not valid on the selected VLANs for the virtual server, or a VIP that is not accessible to your client).

If the Hit Count value increases but no response is received (Server Pkt Count does not increase), the problem is more likely to be in the connectivity between the ACE and the backend real servers. This issue is typically caused by one or more of the following problems:

- You are working on a one-armed configuration (that is, do not plan to change routing for your real servers) and have not selected an appropriate NAT pool for your virtual server to use with source NAT.
- A different routing problem (for example, server traffic does not know how to get back to the ACE).
- Addressing problem (for example, you have an incorrect real server address, or the real server is not accessible to ACE due to network topology).

**Note**

Hit count can increase by more than one, even if you make only a single request from your web browser, because retrieving a typical web page makes many requests from the client to the server.

**Related Topics**

- [Configuring Virtual Servers, page 5-2](#)
- [Information About Using Device Manager to Configure Virtual Servers, page 5-5](#)
- [Virtual Server Usage Guidelines, page 5-6](#)
- [Virtual Server Configuration Procedure, page 5-7](#)

## Virtual Server Configuration Procedure

Use this procedure to add virtual servers to the ACE Appliance Device Manager for load-balancing purposes.

**Assumptions**

- Depending on the protocol to be used for the virtual server, parameter maps need to be defined.
- For SSL service, SSL certificates, keys, chain groups, and parameter maps must be configured.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**.

The Virtual Servers table appears.

- Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, and then click **Edit** to modify it.

The Virtual Server configuration screen appears with a number of configuration subsets. The subsets that you see depend on whether you use the Basic View or the Advanced View and configuration entries you make in the Properties subset. Change views by using the View object selector at the top of the configuration pane.

[Table 5-1](#) identifies and describes virtual server configuration subsets with links to related topics for configuration information.

**Table 5-1** *Virtual Server Configuration Subsets*

| Configuration Subset             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Related Topics                                                                       |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Properties                       | This subset allows you to specify basic virtual server characteristics, such as the virtual server name, IP address, protocol, port, and VLANs.                                                                                                                                                                                                                                                                                                                  | <a href="#">Configuring Virtual Server Properties, page 5-10</a>                     |
| SSL Termination <sup>1</sup>     | This subset appears when TCP is the selected protocol and Other or HTTPS is the application protocol.<br><br>This subset allows you to configure the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients.                                                                                                                                                                                                         | <a href="#">Configuring Virtual Server SSL Termination, page 5-18</a>                |
| Protocol Inspection              | This subset appears in the Advanced View for the following: <ul style="list-style-type: none"> <li>TCP with FTP, HTTP, HTTPS, RTSP, or SIP</li> <li>UDP with DNS or SIP</li> </ul> This subset appears in the Basic view for TCP with FTP.<br><br>This subset allows you to configure the virtual server so that it can verify protocol behavior and identify unwanted or malicious traffic passing through the ACE appliance on selected application protocols. | <a href="#">Configuring Virtual Server Protocol Inspection, page 5-20</a>            |
| L7 Load-Balancing                | This subset appears only in the Advanced View for the following: <ul style="list-style-type: none"> <li>TCP with Generic, HTTP, HTTPS, RTSP, or SIP</li> <li>UDP with Generic, RADIUS, or SIP</li> </ul> This subset allows you to configure Layer 7 load-balancing options, including SSL initiation <sup>1</sup> .                                                                                                                                             | <a href="#">Configuring Virtual Server Layer 7 Load Balancing, page 5-30</a>         |
| Default L7 Load-Balancing Action | This subset allows you to establish the default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions.<br><br>It also allows you to configure SSL initiation <sup>1</sup> . SSL initiation appears only in the Advanced View.                                                                                                                                                                          | <a href="#">Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55</a> |



**Table 5-1** *Virtual Server Configuration Subsets (continued)*

| Configuration Subset                      | Description                                                                                                                                                                                                                        | Related Topics                                                                   |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Application Acceleration And Optimization | This subset appears only in the Advanced View and when HTTP or HTTPS is the selected application protocol.<br><br>This subset allows you to configure application acceleration and optimization options for HTTP or HTTPS traffic. | <a href="#">Configuring Application Acceleration and Optimization, page 5-57</a> |
| NAT                                       | This subset appears in the Advanced View only.<br><br>This subset allows you to set up Name Address Translation (NAT) for the virtual server.                                                                                      | <a href="#">Configuring Virtual Server NAT, page 5-61</a>                        |

1. The SSL initiation and termination configuration options do not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

- Step 3** When you finish configuring virtual server properties, do the following:
- Click **Deploy Now** to deploy the configuration on the ACE appliance.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Virtual Servers table.

- Step 4** (Optional) To display statistics and status information for an existing virtual server, from the Virtual Servers table, choose a virtual server and click **Details**.

A pop-up window appears that displays the detailed virtual server information (see the [“Displaying Virtual Server Statistics and Status Information”](#) section on page 5-62 for details).



**Note** This feature requires ACE software Version A3(2.1) or later. An error displays with earlier software versions.

#### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Understanding Virtual Server Configuration and ACE Appliance Device Manager, page 5-2](#)
- [Information About Using Device Manager to Configure Virtual Servers, page 5-5](#)
- [Shared Objects and Virtual Servers, page 5-9](#)
- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)

## Shared Objects and Virtual Servers

A shared object is one that is used by multiple virtual servers. Examples of shared objects are as follows:

- Action lists
- Class maps
- Parameter maps

- Real servers
- Server farms
- SSL services
- Sticky groups

Because these objects are shared, modifying an object's configuration in one virtual server can impact other virtual servers that use the same object.

### Configuring Shared Objects

ACE Appliance Device Manager offers the following options for shared objects in virtual server configuration screens (**Config > Virtual Contexts > context > Load Balancing > Virtual Servers**):

- **View**—Click **View** to review the object's configuration. The screen refreshes with read-only fields and the following three buttons.
- **Cancel**—Click **Cancel** to close the read-only view and to return to the previous screen.
- **Edit**—Click **Edit** to modify the selected object's configuration. The screen refreshes with fields that can be modified, except for the Name field which remains read-only.



**Note** Before changing a shared object's configuration, make sure you understand the effect of the changes on other virtual servers using the same object. As an alternative, consider using the Duplicate option instead.

- **Duplicate**—Click **Duplicate** to create a new object with the same configuration as the selected object. The screen refreshes with configurable fields. In the Name field, enter a unique name for the new object, and then modify the configuration as desired. This option allows you to create a new object without impacting other virtual servers using the same object.

### Deleting Virtual Servers with Shared Objects

If you create a virtual server and include shared objects in its configuration, deleting the virtual server does not delete the associated shared objects. This ensures that other virtual servers using the same shared objects are not impacted.

### Related Topics

- [Managing Virtual Servers, page 5-63](#)
- [Configuring Virtual Server Properties, page 5-10](#)
- [Configuring Virtual Server SSL Termination, page 5-18](#)
- [Configuring Virtual Server Protocol Inspection, page 5-20](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 5-30](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55](#)
- [Configuring Application Acceleration and Optimization, page 5-57](#)

## Configuring Virtual Server Properties

Use this procedure to configure virtual server properties.


## Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, and then click **Edit** to modify it. The Virtual Server configuration screen appears. The Properties configuration subset is open by default.
- The fields that you see in the Properties configuration subset depend on whether you are using Advanced View or Basic View:
- To configure Advanced View properties, continue with [Step 3](#).
  - To configure Basic View properties, continue with [Step 4](#).
- Step 3** To configure virtual server properties in the Advanced View, enter the information in [Table 5-2](#).

**Table 5-2** *Virtual Server Properties – Advanced View*

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Server Name      | Enter the name for the virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IP Address Type          | Select either IPv4 or IPv6 for the address type of the virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Virtual IP Address       | Enter the IP address for the virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Virtual IP Mask          | (IPv4 address type only) Select the subnet mask to apply to the virtual server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Virtual IP Prefix Length | (IPv6 address type only) Enter the prefix length to apply to the virtual server IP address. The default length for the prefix is 128.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Transport Protocol       | <p>Select the protocol the virtual server supports:</p> <ul style="list-style-type: none"> <li>• Any—Indicates the virtual server is to accept connections using any IP protocol.</li> <li>• TCP—Indicates that the virtual server is to accept connections that use TCP.</li> <li>• UDP—Indicates that the virtual server is to accept connections that use UDP.</li> </ul> <p><b>Note</b> This field is read-only if you are editing an existing virtual server. The Device Manager does not allow changes between protocols that require a change to the Layer 7 server load-balancing policy map. You need to delete the virtual server and create a new one with the desired protocol.</p> |

**Table 5-2** *Virtual Server Properties – Advanced View (continued)*

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Protocol | <p>This field appears if TCP or UDP is selected. Select the application protocol to be supported by the virtual server.</p> <p><b>Note</b> This field is read-only if you are editing an existing virtual server. The Device Manager does not allow changes between protocols that require a change to the Layer 7 server load-balancing policy map. You need to delete the virtual server and create a new one with the desired application protocol.</p> <p>For TCP, the options are as follows:</p> <ul style="list-style-type: none"> <li>FTP—File Transfer Protocol</li> <li>Generic—Generic protocol parsing</li> <li>HTTP—Hyper Text Transfer Protocol</li> <li>HTTPS—HTTP over SSL</li> </ul> <p>If you select HTTPS, the SSL Termination configuration subset appears. See the <a href="#">“Configuring Virtual Server SSL Termination” section on page 5-18</a>.</p> <ul style="list-style-type: none"> <li>Other—Any protocol other than those specified</li> <li>RDP—Remote Desktop Protocol</li> <li>RTSP—Real Time Streaming Protocol</li> <li>SIP—Session Initiation Protocol</li> <li>Unterminated HTTPS</li> </ul> <p></p> <p><b>Note</b> This option is not available if the ACE is using the NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version” section on page 1-2</a>).</p> <p>For UDP, the options are as follows:</p> <ul style="list-style-type: none"> <li>DNS—Domain Name System</li> <li>Generic—Generic protocol parsing</li> <li>Other—Any protocol other than those specified</li> <li>RADIUS—Remote Authentication Dial-In User Service</li> <li>SIP—Session Initiation Protocol</li> </ul> <p>If you select any specific application protocol, the Protocol Inspection configuration subset appears. See the <a href="#">“Configuring Virtual Server Protocol Inspection” section on page 5-20</a>.</p> |

**Table 5-2**      *Virtual Server Properties – Advanced View (continued)*

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port      | <p>By default, this field appears with the default port number for the specified protocol.</p> <p>To change the port number, enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as 10-20. Enter 0 (zero) to indicate all ports.</p> <p>For a complete list of protocols and ports, see the Internet Assigned Numbers Authority available at <a href="http://www.iana.org/numbers/">www.iana.org/numbers/</a>.</p> |
| All VLANs | Check the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.                                                                                                                                                                                                                                                                                                                                                    |

Table 5-2 Virtual Server Properties – Advanced View (continued)

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN                     | <p>This field appears if the All VLANs check box is cleared.</p> <p>In the Available list, select the VLANs to use for incoming traffic, and then click <b>Add to Selection</b>. The items appear in the Selected list.</p> <p>To remove VLANs, select them in the Selected lists and then click <b>Remove from Selection</b>. The items appear in the Available list.</p> <p><b>Note</b> You cannot change the VLAN for a virtual server once it is specified. Instead, you need to delete the virtual server and create a new one with the desired VLAN.</p>                                                                                                                                                                                                                                                                                                                                              |
| HTTP Parameter Map       | <p>This field appears if HTTP or HTTPS is the selected application protocol. Select an existing HTTP parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the “<a href="#">Shared Objects and Virtual Servers</a>” section on page 5-9 for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the HTTP Parameter Map configuration pane appears. Configure the HTTP parameter map as described in <a href="#">Table 8-2</a>.</li> </ul>                                                                                                                                                                                                                                                                        |
| Connection Parameter Map | <p>This field appears if TCP is the selected protocol. Select an existing connection parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the “<a href="#">Shared Objects and Virtual Servers</a>” section on page 5-9 for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the Connection Parameter Map configuration pane appears. Configure the connection parameter map as described in <a href="#">Table 8-3</a>.</li> </ul> <p><b>Note</b> Click <b>More Settings</b> to access the additional Connection Parameter Maps configuration attributes. By default, Device Manager hides the default Connection Parameter Maps configuration attributes and the attributes which are not commonly used.</p> |

Table 5-2 Virtual Server Properties – Advanced View (continued)

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KAL-AP-TAG Name               | <p>The KAL-AP-TAG feature allows the Cisco Global Site Selector (GSS) proprietary KAL-AP protocol to extract load and availability information from the ACE when a firewall is positioned between the GSS and the ACE. This feature allows you to configure a tag (name) per VIP for a maximum of 4,096 tags on an ACE. This feature does not replace the tag per domain feature. For more information about this feature, see the Configuring Health Monitoring chapter in the <i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i>.</p> <p>In the KAL-AP-TAG Name field, enter the name as an unquoted text string with no spaces and a maximum of 76 alphanumeric characters.</p> <p>The following scenarios are not supported and will result in an error:</p> <ul style="list-style-type: none"> <li>You cannot configure a tag name for a VIP that already has a tag configuration as part of a different policy configuration.</li> <li>You cannot associate the same tag name with more than one VIP.</li> <li>You cannot associate the same tag name with a domain and a VIP.</li> <li>You cannot assign two different tags to two different Layer 3 class maps that have the same VIP, but different port numbers. The KAL-AP protocol considers these class maps to have the same VIP and calculates the load for both Layer 3 rules together when the GSS queries the VIP.</li> </ul> |
| Kal-AP Primary Out of Service | <p>Check this box for the ACE to notify the Global Site Selector (GSS) that the primary server farm is down when the backup server farm is in use.</p> <p>By default, when you configure a redirect server farm as a backup server farm on the ACE and the primary server farm fails, the backup server farm redirects the client requests to another data center. However, the VIP remains in the INSERVICE state.</p> <p>When you configure the ACE to communicate with a GSS, it provides information for server availability. When a backup server is in use after the primary server farm is down and this feature is enabled, the ACE informs the GSS that the VIP for the primary server farm is out of service by returning a load value of 255. The GSS recognizes that the primary server farm is down and sends future DNS requests with the IP address of the other data center.</p> <p>Clear this check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| DNS Parameter Map             | <p>This field appears if DNS is the selected protocol over UDP.</p> <p>Select an existing DNS parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the “<a href="#">Shared Objects and Virtual Servers</a>” section on page 5-9 for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the DNS Parameter Map configuration pane appears. Configure the DNS parameter map as described in <a href="#">Table 8-11</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |


Table 5-2 Virtual Server Properties – Advanced View (continued)

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Generic Parameter Map | <p>This field appears if Generic is the selected application protocol over TCP or UDP.</p> <p>Select an existing Generic parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the “<a href="#">Shared Objects and Virtual Servers</a>” section on page 5-9 for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the Generic Parameter Map configuration pane appears. Configure the Generic parameter map as described in <a href="#">Table 8-7</a>.</li> </ul>                                                                                                                            |
| RTSP Parameter Map    | <p>This field appears if RTSP is the selected application protocol over TCP.</p> <p>Select an existing RTSP parameter map or click <b>*New*</b> to create a new one:</p> <ul style="list-style-type: none"> <li>If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See the “<a href="#">Shared Objects and Virtual Servers</a>” section on page 5-9 for more information about modifying shared objects.</li> <li>If you click <b>*New*</b>, the RTSP Parameter Map configuration pane appears. Configure the RTSP parameter map as described in <a href="#">Table 8-8</a>.</li> </ul>                                                                                                                                               |
| ICMP Reply            | <p>Indicate how the virtual server is to respond to ICMP ECHO requests:</p> <ul style="list-style-type: none"> <li>None—Indicates that the virtual server is not to send ICMP ECHO-REPLY responses to ICMP requests.</li> <li>Active—Indicates that the virtual server is to send ICMP ECHO-REPLY responses only if the configured VIP is active.</li> <li>Always—Indicates that the virtual server is always to send ICMP ECHO-REPLY responses to ICMP requests.</li> <li>Primary Inservice—The virtual server is to reply to an ICMP ping only if the primary server farm state is UP, regardless of the state of the backup server farm. If this option is selected and the primary server farm state is DOWN, the ACE discards the ICMP request and the request times out.</li> </ul> |
| Status                | <p>Indicate whether the virtual server is to be in service or out of service:</p> <ul style="list-style-type: none"> <li>In Service—Enables the virtual server for load-balancing operations.</li> <li>Out Of Service—Disables the virtual server for load-balancing operations.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Step 4** To configure virtual server properties in the Basic View, enter the information in [Table 5-3](#).



Table 5-3 Virtual Server Properties – Basic View

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Server Name  | Enter the name for the virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IP Address Type      | Select either IPv4 or IPv6 for the address type of the virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Virtual IP Address   | Enter the IP address for the virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Transport Protocol   | <p>Select the protocol that the virtual server supports:</p> <ul style="list-style-type: none"> <li>Any—Indicates that the virtual server is to accept connections using any IP protocol.</li> <li>TCP—Indicates that the virtual server is to accept connections that use TCP.</li> <li>UDP—Indicates that the virtual server is to accept connections that use UDP.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Application Protocol | <p>Select the application protocol to be supported by the virtual server.</p> <p>For TCP, the options as follows:</p> <ul style="list-style-type: none"> <li>FTP—File Transfer Protocol</li> <li>HTTP—Hyper Text Transfer Protocol</li> <li>HTTPS—HTTP over SSL</li> </ul> <p>If you select HTTPS, the SSL Termination configuration subset appears. See the <a href="#">“Configuring Virtual Server SSL Termination”</a> section on page 5-18.</p> <div>  <p><b>Note</b> This option is not available if the ACE is using the NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> </div> <ul style="list-style-type: none"> <li>Generic—Generic protocol parsing</li> <li>Other—Any protocol other than those specified.</li> <li>RTSP—Real Time Streaming Protocol</li> <li>RDP—Remote Desktop Protocol</li> <li>SIP—Session Initiation Protocol</li> </ul> <p>For UDP, the options as follows:</p> <ul style="list-style-type: none"> <li>DNS—Domain Name System</li> <li>Generic—Generic protocol parsing</li> <li>Other—Any protocol other than those specified.</li> <li>RTSP—Real Time Streaming Protocol</li> <li>RADIUS—Remote Authentication Dial-In User Service</li> <li>SIP—Session Initiation Protocol</li> </ul> |

**Table 5-3** *Virtual Server Properties – Basic View (continued)*

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port      | <p>By default, this field appears with the default port number for the specified protocol.</p> <p>To change the port number, enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as 10-20. Enter 0 (zero) to indicate all ports.</p> <p>For a complete list of all protocols and ports, see the Internet Assigned Numbers Authority available at <a href="http://www.iana.org/numbers/">www.iana.org/numbers/</a>.</p>                                                                |
| All VLANs | Check the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| VLAN      | <p>This field appears if the All VLANs check box is cleared.</p> <p>In the Available list, select the VLANs to use for incoming traffic, and then click <b>Add to Selection</b>. The items appear in the Selected list.</p> <p>To remove VLANs, select them in the Selected lists, and then click <b>Remove from Selection</b>. The items appear in the Available list.</p> <p><b>Note</b> You cannot change the VLAN for a virtual server once it is specified. Instead, you need to delete the virtual server and create a new one with the desired VLAN.</p> |

**Step 5** When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy the configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries.

#### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Configuring Virtual Server SSL Termination, page 5-18](#)

## Configuring Virtual Server SSL Termination



#### Note

The information in this section does not apply to the ACE NPE software version (see the “[Information About the ACE No Payload Encryption Software Version](#)” section on page 1-2).

SSL termination service allows the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients and then establishes a TCP connection to an HTTP server. When the ACE terminates the SSL connection, it decrypts the ciphertext from the client and transmits the data as clear text to an HTTP server.

Use this procedure to configure virtual server SSL termination service.

**Assumption**

A virtual server has been configured for HTTPS over TCP or Other over TCP in the Properties configuration subset. For more information, see the [“Configuring Virtual Server Properties” section on page 5-10](#).

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for SSL termination, and then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **SSL Termination**. The Proxy Service Name field appears.
- Step 4** In the Proxy Service Name field, select an existing SSL termination service, or select **\*New\*** to create a new SSL proxy service:
  - If you select an existing SSL service, the screen refreshes and allows you to view, modify, or duplicate the existing configuration. See the [“Shared Objects and Virtual Servers” section on page 5-9](#) for more information about modifying shared objects.
  - If you select **\*New\***, the Proxy Service configuration subset appears.
- Step 5** Configure the SSL service using the in [Table 5-4](#).

**Table 5-4** *Virtual Server SSL Termination Attributes*

| Field           | Description                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | Enter a name for this SSL proxy service. Valid entries are alphanumeric strings with a maximum of 64 characters.                                                                                                                                                                                                               |
| Keys            | Select the SSL key pair to use during the SSL handshake for data encryption.                                                                                                                                                                                                                                                   |
| Certificates    | Select the SSL certificate to use during the SSL handshake.                                                                                                                                                                                                                                                                    |
| Chain Groups    | Select the chain group to use during the SSL handshake.                                                                                                                                                                                                                                                                        |
| Auth Groups     | Select the SSL authentication group to associate with this proxy server service.                                                                                                                                                                                                                                               |
| CRL Best-Effort | This option appears if you select an authentication group in the Auth Group Name field.<br><br>Check the check box to allow the ACE to search client certificates for the service to determine if it contains a CRL in the extension and retrieve the value, if it exists.<br><br>Clear the check box to disable this feature. |
| CRL Name        | This option appears if the CRL Best-Effort check box is clear.<br><br>Select the Certificate Revocation List if the ACE is to use for this proxy service.                                                                                                                                                                      |
| Parameter Maps  | Select the SSL parameter map to associate with this proxy server service.                                                                                                                                                                                                                                                      |

For more information about SSL, see the [“Configuring SSL” section on page 9-1](#).

- Step 6** When you finish configuring virtual server properties, do the following:
  - Click **Deploy Now** to deploy this configuration on the ACE appliance.

- Click **Cancel** to exit this procedure without saving your entries.
- 

#### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Configuring Virtual Server Properties, page 5-10](#)

## Configuring Virtual Server Protocol Inspection

Configuring protocol inspection allows the virtual server to verify protocol behavior and identify unwanted or malicious traffic passing through the ACE appliance.

In the Advanced View, protocol inspection configuration is available for the following virtual server protocol configurations:

- TCP with FTP, HTTP, HTTPS, RTSP, or SIP
- UDP with DNS or SIP

In the Basic View, protocol inspection configuration is available for TCP with FTP.

Use this procedure to configure protocol inspection on a virtual server.

#### Assumption

A virtual server has been configured to use one of the protocols that supports protocol inspection in the Properties configuration subset. See the “[Configuring Virtual Server Properties](#)” section on page 5-10 for information on configuring these protocols.

#### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
  - Step 2** Select the virtual server that you want to configure for protocol inspection, and then click **Edit**. The Virtual Server configuration screen appears.
  - Step 3** Click **Protocol Inspection**. The Enable Inspect check box appears.
  - Step 4** Check the Enable Inspect check box to enable inspection on the specified traffic. Clear this check box to disable inspection on this traffic. By default, ACE appliances allow all request methods.
  - Step 5** If you checked the Enable Inspect check box, configure additional inspection options according to virtual server application protocol configuration:
    - For DNS, in the Length field enter the maximum length of the DNS packet in bytes. Valid entries are from 512 to 65535 bytes. If you do not enter a value in this field, the DNS packet size is not checked.
    - For FTP, continue with [Step 6](#).
    - For HTTP and HTTPS, continue with [Step 7](#).
    - For SIP, continue with [Step 9](#).



#### Note

There are no protocol-specific inspection options for RTSP.

---

- Step 6** For FTP protocol inspection, do the following:
- Check the Use Strict check box to indicate that the virtual server is to perform enhanced inspection of FTP traffic and enforce compliance with RFC standards. Clear this check box to indicate that the virtual server is not to perform enhanced FTP inspection.
  - If you checked the Use Strict check box, in the Blocked FTP Commands field, identify the commands that are to be denied by the virtual server. See [Table 12-13](#) for more information about the FTP commands.
    - Select the commands that are to be blocked by the virtual server in the Available list, and then click **Add**. The commands appear in the Selected list.
    - To remove commands that you do not want to be blocked, select them in the Selected list, and then click **Remove**. The commands appear in the Available list.
- Step 7** For HTTP or HTTPS inspection, do the following:
- Check the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic.
  - In the Policy subset, click **Add** to add a new match condition and action, or select an existing match condition and action, and then click **Edit** to modify it. The Policy configuration pane appears.
  - In the Matches field, select an existing class map or **\*New\*** or **\*Inline Match\*** to configure new match criteria for protocol inspection.
- If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See the “[Shared Objects and Virtual Servers](#)” section on [page 5-9](#) for more information about modifying shared objects.
- Configure match criteria and related actions by following the steps in [Table 5-5](#).

**Table 5-5** Protocol Inspection Match Criteria Configuration

| Selection          | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Existing class map | <ol style="list-style-type: none"> <li>Click <b>View</b> to review the match condition information for the selected class map.</li> <li>Do the following:           <ul style="list-style-type: none"> <li>Click <b>Cancel</b> to continue without making changes and to return to the previous screen.</li> <li>Click <b>Edit</b> to modify the existing configuration.</li> <li>Click <b>Duplicate</b> to create a new class map with the same attributes without affecting other virtual servers using the same class map.</li> </ul> <p>See the “<a href="#">Shared Objects and Virtual Servers</a>” section on <a href="#">page 5-9</a> for more information about modifying shared objects.</p> </li> <li>In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria:           <ul style="list-style-type: none"> <li>Permit—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria.</li> <li>Reset—Indicates that the specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.</li> </ul> </li> </ol> |

Table 5-5 Protocol Inspection Match Criteria Configuration (continued)

| Selection             | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>*New*</b>          | <ol style="list-style-type: none"> <li>1. In the Name field, specify a unique name for this class map.</li> <li>2. In the Match field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> <li>– All—Indicates that a match exists only if all match conditions are satisfied.</li> <li>– Any—Indicates that a match exists if at least one of the match conditions is satisfied.</li> </ul> </li> <li>3. In the Conditions table, click <b>Add</b> to add a new set of conditions, or select an existing entry, and then click <b>Edit</b> to modify it. The Type field appears.</li> <li>4. In the Type field, select the type of condition that is to be met for protocol inspection and configure protocol-specific criteria using the information in <a href="#">Table 5-6</a>.</li> <li>5. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> <li>– Permit—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria.</li> <li>– Reset—Indicates that the specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.</li> </ul> </li> </ol> |
| <b>*Inline Match*</b> | <ol style="list-style-type: none"> <li>1. In the Conditions Type field, select the type of inline match condition that is to be met for protocol inspection.<br/><a href="#">Table 5-6</a> describes the types of conditions and their related configuration options.</li> <li>2. Provide condition-specific criteria using the information in <a href="#">Table 5-6</a>.</li> <li>3. In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: <ul style="list-style-type: none"> <li>– Permit—Indicates that the specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria.</li> <li>– Reset—Indicates that the specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.</li> </ul> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Table 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options

| Condition                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content                   | <p>Specific content contained within the HTTP entity-body is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255 bytes.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Content Length            | <p>The content parse length is used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Content Length Operator field, select the operand to use to compare content length: <ul style="list-style-type: none"> <li>– Equal To—The content length must equal the number in the Content Length Value field.</li> <li>– Greater Than—The content length must be greater than the number in the Content Length Value field.</li> <li>– Less Than—The content length must be less than the number in the Content Length Value field.</li> <li>– Range—The content length must be within the range specified in the Content Length Lower Value field and the Content Length Higher Value field.</li> </ul> </li> <li>2. Enter values to apply for content length comparison: <ul style="list-style-type: none"> <li>– If you select Equal To, Greater Than, or Less Than in the Content Length Operator field, the Content Length Value field appears. In the Content Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 4294967295.</li> <li>– If you select Range in the Content Length Operator field, the Content Length Lower Value and the Content Length Higher Value fields appear: <ol style="list-style-type: none"> <li>1. In the Content Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value field.</li> <li>2. In the Content Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value field.</li> </ol> </li> </ul> </li> </ol> |
| Content Type Verification | <p>Verification of MIME-type messages with the header MIME-type is to be used for application inspection decisions. This option verifies that the header MIME-type value is in the internal list of supported MIME-types and that the header MIME-type matches the content in the data or body portion of the message.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Table 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

| Condition        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Header           | <p>The name and value in an HTTP header are used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Header field, select one of the predefined HTTP headers to match, or select HTTP Header to specify a different HTTP header.</li> <li>2. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>3. In the Header Value field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Header Length    | <p>The length of the header in the HTTP message is used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: <ul style="list-style-type: none"> <li>– Request—HTTP header request messages are to be checked for header length.</li> <li>– Response—HTTP header response messages are to be checked for header length.</li> </ul> </li> <li>2. In the Header Length Operator field, select the operand to be used to compare header length: <ul style="list-style-type: none"> <li>– Equal To—The header length must equal the number in the Header Length Value field.</li> <li>– Greater Than—The header length must be greater than the number in the Header Length Value field.</li> <li>– Less Than—The header length must be less than the number in the Header Length Value field.</li> <li>– Range—The header length must be within the range specified in the Header Length Lower Value field and the Header Length Higher Value field.</li> </ul> </li> <li>3. Enter values to apply for header length comparison: <ul style="list-style-type: none"> <li>– If you select Equal To, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value field appears. In the Header Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 255.</li> <li>– If you select Range in the Header Length Operator field, the Header Length Lower Value and the Header Length Higher Value fields appear: <ol style="list-style-type: none"> <li>1. In the Header Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value field.</li> <li>2. In the Header Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value field.</li> </ol> </li> </ul> </li> </ol> |
| Header MIME Type | <p>Multipurpose Internet Mail Extension (MIME) message types are used for application inspection decisions.</p> <p>In the Header MIME Type field, select the MIME message type to use for this match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



Table 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

| Condition         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Misuse       | <p>The misuse of port 80 (or any other port running HTTP) is to be used for application inspection decisions.</p> <p>Indicate the application category to use for this match condition:</p> <ul style="list-style-type: none"> <li>• IM—Instant messaging applications are to be checked.</li> <li>• P2P—Peer-to-peer applications are to be checked.</li> <li>• Tunneling—Tunneling applications are to be checked.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Request Method    | <p>A request method is to be used for protocol inspection decisions. By default, the ACE allows all request and extension methods. This option allows you to configure protocol inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods.</p> <ol style="list-style-type: none"> <li>1. Select the type of request method to use for this match condition: <ul style="list-style-type: none"> <li>– Ext—An HTTP extension method is to be used.</li> </ul> <div data-bbox="516 772 565 814" data-label="Image"></div> <div data-bbox="509 814 571 842" data-label="Section-Header"><b>Note</b></div> <div data-bbox="597 814 1450 877" data-label="Text"> <p>The list of available HTTP extension methods from which to choose varies depending on the version of software installed in the ACE.</p> </div> <ul style="list-style-type: none"> <li>– RFC—The request method defined in RFC 2616 is to be used.</li> </ul> </li> <li>2. In the Request Method field, select the request method that is to be inspected.</li> </ol> |
| Strict HTTP       | Compliance with HTTP RFC 2616 is to be used for application inspection decisions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Transfer Encoding | <p>An HTTP transfer-encoding type is to be used for application inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient.</p> <p>In the Transfer Encoding field, select the type of encoding that is to be checked:</p> <ul style="list-style-type: none"> <li>• Chunked—The message body is transferred as a series of chunks.</li> <li>• Compress—The encoding format that is produced by the UNIX file compression program <i>compress</i>.</li> <li>• Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951.</li> <li>• Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952.</li> <li>• Identity—The default (identity) encoding which does not require the use of transformation.</li> </ul>                                                                             |

Table 5-6 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

| Condition  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL        | <p>URL names are to be used for application inspection decisions.</p> <p>In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| URL Length | <p>URL length is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>In the URL Length Operator field, select the operand to use to compare URL length: <ul style="list-style-type: none"> <li>Equal To—The URL length must equal the number in the URL Length Value field.</li> <li>Greater Than—The URL length must be greater than the number in the URL Length Value field.</li> <li>Less Than—The URL length must be less than the number in the URL Length Value field.</li> <li>Range—The URL length must be within the range specified in the URL Length Lower Value field and the URL Length Higher Value field.</li> </ul> </li> <li>Enter values to apply for URL length comparison: <ul style="list-style-type: none"> <li>If you select Equal To, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value field appears. In the URL Length Value field, enter the value for comparison. Valid entries are from 1 to 65535 bytes.</li> <li>If you select Range in the URL Length Operator field, the URL Length Lower Value and the URL Length Higher Value fields appear: <ol style="list-style-type: none"> <li>In the URL Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value field.</li> <li>In the URL Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value field.</li> </ol> </li> </ul> </li> </ol> |

- e. Do the following:
  - Click **OK** to save your entries. The Conditions table refreshes with the new entry.
  - Click **Cancel** to exit the Policy subset without saving your entries.
- f. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for protocol inspection are not met:
  - Permit—Indicates that the specified HTTP traffic is to be received by the virtual server.
  - Reset—Indicates that the specified HTTP traffic is to be denied by the virtual server.
  - N/A—Indicates that this attribute is not set.

**Step 8** For SIP inspection, do the following:

- a. In the Actions subset, click **Add** to add a new match condition and action, or select an existing match condition and action, and then click **Edit** to modify it. The Actions configuration pane appears.
- b. In the Matches field, select an existing class map or **\*New\*** or **\*Inline Match\*** to configure new match criteria for protocol inspection.

If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See the “[Shared Objects and Virtual Servers](#)” section on page 5-9 for more information about modifying shared objects.

- c. Configure match criteria and related actions using the information in [Table 5-7](#).

**Table 5-7** *SIP Protocol Inspection Conditions and Options*

| Condition        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Called Party     | <p>The destination or called party specified in the URI of the SIP To header is used for SIP protocol inspection decisions.</p> <p>In the Called Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                                                                                                                                           |
| Calling Party    | <p>The source or caller specified in the URI of the SIP From header is used for SIP protocol inspection decisions.</p> <p>In the Calling Party field, enter a regular expression that identifies the calling party in the URI of the SIP From header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                                                                                                                                                |
| IM Subscriber    | <p>An IM (instant messaging) subscriber is used for application inspection decisions.</p> <p>In the IP Subscriber field, enter a regular expression that identifies the IM subscriber for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                                                                                                                                                                                                               |
| Message Path     | <p>SIP inspection allows you to filter messages coming from or transiting through certain SIP proxy servers. The ACE maintains a list of the unauthorized SIP proxy IP addresses or URIs in the form of regular expressions and checks this list against the VIA header field in each SIP packet.</p> <p>In the Message Path field, enter a regular expression that identifies the SIP proxy server for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> |
| SIP Content Type | <p>The content type in the SIP message body is used for SIP protocol inspection decisions.</p> <p>In the Content Type field, enter a regular expression that identifies the content type in the SIP message body to use for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                                                                                                                                                                             |

Table 5-7 SIP Protocol Inspection Conditions and Options (continued)

| Condition          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIP Content Length | <p>The SIP message body content length is used for SIP protocol inspection decisions.</p> <p>To specify SIP traffic based on SIP message body length:</p> <ol style="list-style-type: none"> <li>1. In the Content Operator field, confirm that Greater Than is selected.</li> <li>2. In the Content Length field, enter the maximum size of a SIP message body in bytes that the ACE is to allow without performing SIP protocol inspection. If a SIP message exceeds the specified value, the ACE performs SIP protocol inspection as defined in an associated policy map. Valid entries are integers from 0 to 65534 bytes.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SIP Request Method | <p>A SIP request method is used for application inspection decisions.</p> <p>In the Request Method field, select the request method that is to be inspected.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Third Party        | <p>SIP allows users to register other users on their behalf by sending REGISTER messages with different values in the From and To header fields. This process can pose a security threat if the REGISTER message is actually a Deregister message. A malicious user could cause a DoS (denial-of-service) attack by deregistering all users on their behalf. To prevent this security threat, you can specify a list of privileged users who can register or unregister someone else on their behalf. The ACE maintains the list as a regex table. If you configure this policy, the ACE drops REGISTER messages with mismatched From and To headers and a From header value that does not match any of the privileged user IDs.</p> <p>In the Third Party Registration Entities field, enter a regular expression that identifies a privileged user who is authorized for third-party registrations. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> |
| URI Length         | <p>The ACE can validate the length of SIP URIs or Tel URIs. A SIP URI is a user identifier that a calling party (source) uses to contact the called party (destination). A Tel URI is a telephone number that identifies the endpoint of a SIP connection. For more information about SIP URIs and Tel URIs, see RFC 2534 and RFC 3966, respectively.</p> <p>To filter SIP traffic based on URIs, do the following:</p> <ol style="list-style-type: none"> <li>1. In the URI Type field, indicate the type of URI to be used: <ul style="list-style-type: none"> <li>– SIP URI—The calling party URI is to be used for this match condition.</li> <li>– Tel URI—A telephone number is to be used for this match condition.</li> </ul> </li> <li>2. In the URI Operator field, confirm that Greater Than is selected.</li> <li>3. In the URI Length field, enter the maximum length of the SIP URI or Tel URI in bytes. Valid entries are integers from 0 to 254 bytes.</li> </ol>                                                                                                                                                                                                                 |

- d. In the Action field, select the action that the virtual server is to take when the specified match conditions are met:
  - Drop—The specified SIP traffic is to be discarded by the virtual server.
  - Permit—The specified SIP traffic is to be received by the virtual server.
  - Reset—The specified SIP traffic is to be denied by the virtual server.
- e. Do the following:
  - Click **OK** to save your entries. The Conditions table refreshes with the new entry.
  - Click **Cancel** to exit the Conditions subset without saving your entries and to return to the Conditions table.
- f. In the SIP Parameter Map field, select an existing parameter map or select **\*New\*** to configure a new one.

If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See the “[Shared Objects and Virtual Servers](#)” section on page 5-9 for more information about modifying shared objects.
- g. Configure SIP parameter map options using the information in [Table 8-9](#).
- h. In the Secondary Connection Parameter Map field, select an existing parameter map or select **\*New\*** to configure a new one.

If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See the “[Shared Objects and Virtual Servers](#)” section on page 5-9 for more information about modifying shared objects.
- i. Configure secondary connection parameter map options using the information in [Table 8-3](#).
- j. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for SIP protocol inspection are not met:
  - Drop—The specified SIP traffic is to be discarded by the virtual server.
  - Permit—The specified SIP traffic is to be received by the virtual server.
  - Reset—The specified SIP traffic is to be denied by the virtual server.
- k. Check the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic.

**Step 9** When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.

---

#### Related Topics

- [Configuring Virtual Server Properties, page 5-10](#)
- [Configuring Virtual Server SSL Termination, page 5-18](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 5-30](#)

## Configuring Virtual Server Layer 7 Load Balancing

Layer 7 load balancing is available for virtual servers configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

See the “[Configuring Virtual Server Properties](#)” section on page 5-10 for information on configuring these protocols.

Use this procedure to configure Layer 7 load balancing on a virtual server.

### Assumption

A virtual server has been configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**.  
The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for Layer 7 load balancing, and then click **Edit**.  
The Virtual Server configuration screen appears.
- Step 3** Click **L7 Load-Balancing**. The Layer 7 Load-Balancing Rule Match table appears.
- Step 4** In the Rule Match table, click **Add** to add a new match condition and action, or select an existing match condition and action, and then click **Edit** to modify it.  
The Rule Match configuration pane appears.
- Step 5** In the Rule Match field, select an existing class map or **\*New\*** or **\*Inline Match\*** to configure new match criteria for Layer 7 load balancing:
- If you select an existing class map, click **View** to review, modify, or duplicate the existing configuration. See the “[Shared Objects and Virtual Servers](#)” section on page 5-9 for more information about modifying shared objects.
  - If you click **\*New\*** or **\*Inline Match\***, the Rule Match configuration subset appears.
- Step 6** Configure match criteria by following the steps in [Table 5-8](#).

**Table 5-8** *Layer 7 Load-Balancing Match Criteria Configuration*

| Selection             | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Existing class map    | <ol style="list-style-type: none"> <li>Click <b>View</b> to review the match condition information for the selected class map.</li> <li>Do the following: <ul style="list-style-type: none"> <li>Click <b>Cancel</b> to continue without making changes and to return to the previous screen.</li> <li>Click <b>Edit</b> to modify the existing configuration.</li> <li>Click <b>Duplicate</b> to create a new class map with the same attributes without affecting other virtual servers using the same class map.</li> </ul> </li> </ol> <p>See the “<a href="#">Shared Objects and Virtual Servers</a>” section on page 5-9 for more information about modifying shared objects.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>*New*</b>          | <ol style="list-style-type: none"> <li>In the Name field, enter a unique name for this class map.</li> <li>In the Matches field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> <li>Any—Indicates that a match exists if at least one of the match conditions is satisfied.</li> <li>All—Indicates that a match exists only if all match conditions are satisfied.</li> </ul> </li> <li>In the Conditions table, click <b>Add</b> to add a new set of conditions or select an existing entry, and then click <b>Edit</b> to modify it.</li> <li>In the Type field, select the match condition and configure any protocol-specific options: <ul style="list-style-type: none"> <li>For Generic protocol options, see <a href="#">Table 12-8</a>.</li> <li>For HTTP and HTTPS protocol options, see <a href="#">Table 5-9</a>.</li> <li>For RADIUS protocol options, see <a href="#">Table 12-9</a>.</li> <li>For RTSP protocol options, see <a href="#">Table 12-10</a>.</li> <li>For SIP protocol options, see <a href="#">Table 12-11</a>.</li> </ul> </li> <li>Configure any condition-specific options using the information in <a href="#">Table 5-9</a>.</li> <li>Do the following: <ul style="list-style-type: none"> <li>Click <b>OK</b> to accept your entries and to return to the Conditions table.</li> <li>Click <b>Cancel</b> to exit this procedure without saving your entries and to return to the Conditions table.</li> </ul> </li> </ol> |
| <b>*Inline Match*</b> | <p>In the Conditions Type field, select the type of inline match condition and configure any protocol-specific options:</p> <ul style="list-style-type: none"> <li>For Generic protocol options, see <a href="#">Table 12-8</a></li> <li>For HTTP and HTTPS protocol options, see <a href="#">Table 5-9</a></li> <li>For RADIUS protocol options, see <a href="#">Table 12-9</a></li> <li>For RTSP protocol options, see <a href="#">Table 12-10</a></li> <li>For SIP protocol options, see <a href="#">Table 12-11</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 5-9 Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration


| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>Indicates that this rule is to use an existing class map to establish match conditions.</p> <p>If you select this method, in the Class Map field, select the class map to be used.</p> <p><b>Note</b> This option is not available for inline match conditions.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| HTTP Content    | <p>Specific content contained within the HTTP entity-body is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| HTTP Cookie     | <p>Indicates that HTTP cookies are to be used for this rule.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</li> <li>3. Check the Secondary Cookie Matching check box to indicate that the ACE appliance is to use both the cookie name and the cookie value to satisfy this match condition. Clear this check box to indicate that the ACE appliance is to use either the cookie name or the cookie value to satisfy this match condition.</li> </ol> |
| HTTP Header     | <p>Indicates that the HTTP header and a corresponding value are to be used for this rule.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the Header Name field, enter the name of the generic field in the HTTP header. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>2. In the Header Value field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. <a href="#">Table 12-33</a> lists the supported characters that you can use in regular expressions.</li> </ol>                                                                                                                  |



**Table 5-9**      *Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration (continued)*

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP URL        | <p>Indicates that this rule is to perform regular expression matching against the received packet data from a particular connections based on the HTTP URL string.</p> <p>If you select this method:</p> <ol style="list-style-type: none"><li>1. In the URL Expression field, enter a URL, or portion of a URL, to match. Valid entries are URL strings from 1 to 255 alphanumeric characters. Include only the portion of the URL following <code>www.hostname.domain</code> in the match statement. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>. To match the <code>www.anydomain.com</code> portion, the URL string can take the form of a URL regular expression. The ACE appliance supports regular expressions for matching URL strings. <a href="#">Table 12-33</a> lists the supported characters that you can use in regular expressions.</li><li>2. In the Method Expression field, enter the HTTP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).</li></ol> |

Table 5-9 Layer 7 HTTP/HTTPS Load-Balancing Rule Match Configuration (continued)

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source Address  | <p>Indicates that this rule is to use a client source IP address to establish match conditions.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the Source Address field, enter the source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).</li> <li>2. In the Netmask field, select the subnet mask to apply to the source IP address.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSL             | <div>  <p><b>Note</b> The SSL option does not apply to the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> </div> <p>Defines load balancing decisions based on the specific SSL cipher or cipher strength. Enables the ACE to load balance client traffic to different server farms based on the SSL encryption level negotiated with the ACE during SSL termination.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the SSL Cipher Match Type field, select the match type. Options are as follows: <ul style="list-style-type: none"> <li>– Equal To—Specifies an SSL cipher for the load balancing decision.</li> <li>– Less Than—Specifies SSL cipher strength for the load balancing decision.</li> </ul> </li> <li>2. If you selected Equal To, in the Cipher Name field specify an SSL cipher for the load balancing decision. The possible values are as follows: <ul style="list-style-type: none"> <li>– RSA_EXPORT1024_WITH_DES_CBC_SHA</li> <li>– RSA_EXPORT1024_WITH_RC4_56_MD5</li> <li>– RSA_EXPORT1024_WITH_RC4_56_SHA</li> <li>– RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>– RSA_EXPORT_WITH_RC4_40_MD5</li> <li>– RSA_WITH_3DES_EDE_CBC_SHA</li> <li>– RSA_WITH_AES_128_CBC_SHA</li> <li>– RSA_WITH_AES_256_CBC_SHA</li> <li>– RSA_WITH_DES_CBC_SHA</li> <li>– RSA_WITH_RC4_128_MD5</li> <li>– RSA_WITH_RC4_128_SHA</li> </ul> </li> <li>3. If you selected Less Than, in the Specify Minimum Cipher Strength field specify a non-inclusive minimum SSL cipher bit strength. For example, if you specify a cipher strength value of 128, any SSL cipher that was no greater than 128 would hit the traffic policy. If the SSL cipher was 128-bit or greater, the connection would miss the policy.</li> </ol> <p>The possible values are as follows:</p> <ul style="list-style-type: none"> <li>– 128—128-bit strength</li> <li>– 168—168-bit strength</li> <li>– 256—256-bit strength</li> <li>– 56—56-bit strength</li> </ul> |

- Step 7** In the Primary Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria:
- **Drop**—Indicates that client requests for content are to be discarded when match conditions are met. Continue with [Step 10](#).
  - **Forward**—Indicates that client requests for content are to be forwarded without performing load balancing on the requests when match conditions are met. Continue with [Step 10](#).
  - **Load Balance**—Indicates that client requests for content are to be directed to a server farm when match conditions are met. Continue with [Step 8](#).
  - **Sticky**—Client requests for content are handled by a sticky group when match conditions are met. Continue with [Step 8](#).
- Step 8** If you select Load Balance as the primary action, you can configure load balancing using a server farm, a server farm/backup server farm pair, an existing sticky group, or a new sticky group.
- If you select an existing object in any of these scenarios, you can view, modify, or duplicate the selected object's existing configuration. See the “[Shared Objects and Virtual Servers](#)” section on page 5-9 for more information about modifying shared objects in virtual servers.

**Note**

To display statistics and status information for an existing server farm, choose a server farm in the list, and click **Details**. DM accesses the **show serverfarm name detail** CLI command to display detailed server farm information. See the “[Displaying Server Farm Statistics and Status Information](#)” section on page 6-39.

Configure load balancing using the information in [Table 5-10](#).

**Table 5-10**      *Virtual Server Load-Balancing Options*

| To configure...                                            | Do this...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Load balancing using a server farm                         | In the Server Farm field, select the server farm <sup>1</sup> to be used for load balancing for this virtual server, or select <b>*New*</b> to configure a new server farm (see <a href="#">Table 5-11</a> ).                                                                                                                                                                                                                                                                                                              |
| Load balancing using a server farm/backup server farm pair | <ol style="list-style-type: none"> <li>1. In the Server Farm field, select the primary server farm<sup>1</sup> to use for load balancing, or select <b>*New*</b> to configure a new server farm (see <a href="#">Table 5-11</a>).</li> <li>2. In the Backup Server Farm field, select the server farm<sup>1</sup> to act as the backup server farm for load balancing if the primary server farm is unavailable, or select <b>*New*</b> to configure a new backup server farm (see <a href="#">Table 5-11</a>).</li> </ol> |

Table 5-10 Virtual Server Load-Balancing Options (continued)

| To configure...                               | Do this...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Load balancing using an existing sticky group | <ol style="list-style-type: none"> <li>1. In the Server Farm field, select the primary server farm<sup>1</sup> to use for load balancing. This must be the primary server farm specified in the existing sticky group.</li> <li>2. In the Backup Server Farm field, select the backup server farm<sup>1</sup> to use for load balancing. This must be the backup server farm specified in the existing sticky group.</li> <li>3. In the Sticky Group field, select the sticky group to use.</li> </ol> <p><b>Note</b> Sticky groups appear in the Sticky Group field <b>only</b> when their configured primary and backup server farms are selected, respectively. If you select a sticky group and then select a different primary or backup server farm, the sticky group that you selected in the Sticky Group field no longer appears. To change an existing sticky group configuration, modify it in the Stickiness configuration screen (<b>Config &gt; Virtual Contexts &gt; context &gt; Load Balancing &gt; Stickiness</b>).</p> |
| Load balancing using a new sticky group       | <ol style="list-style-type: none"> <li>1. In the Server Farm field, select the primary server farm<sup>1</sup> to use for load balancing, or select <b>*New*</b> to configure a new server farm (see <a href="#">Table 5-11</a>).</li> <li>2. In the Backup Server Farm field, select the server farm<sup>1</sup> to act as the backup server farm for load balancing if the primary server farm is unavailable, or select <b>*New*</b> to configure a new backup server farm (see <a href="#">Table 5-11</a>).</li> <li>3. In the Sticky Group field, select <b>*New*</b>, and then configure a new sticky group using the information in <a href="#">Table 5-13</a>.</li> </ol> <p><b>Note</b> The context in which you configure a sticky group must be associated with a resource class that allocates a portion of ACE appliance resources to stickiness. See the “<a href="#">Managing Resource Classes</a>” section on page 4-35 for more information on resource classes.</p>                                                     |

1. When you select an existing server farm, you can do the following using the function buttons that appear:
- Click **View** to display the server farm configuration, which you can then edit or duplicate using the functions buttons that appear.
  - Click **Details** to display the **show serverfarm sf\_name detail** command output in a pop-up window. This command output provides server farm configuration information.
  - Click **Buddy Group** to display the **show buddy group** command output in a pop-up window. This command output shows the list of buddy groups that are configured in the virtual context (for more information, see the “[Buddy Sticky Groups](#)” section on page 7-6).

**Table 5-11** *New Server Farm Attributes*

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | Enter a unique name for this server farm. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Type        | <p>Select the type of server farm:</p> <ul style="list-style-type: none"> <li>• <b>Host</b>—A typical server farm that consists of real servers that provide content and services to clients. By default, if you configure a backup server farm and all real servers in the primary server farm go down, the primary server farm fails over to the backup server farm. Use the following options to specify thresholds for failover and returning to service. <ul style="list-style-type: none"> <li>a. In the Partial-Threshold Percentage field, enter the minimum percentage of real servers in the primary server farm that must remain active for the server farm to stay up. If the percentage of active real servers falls below this threshold, the ACE takes the server farm out of service. Valid entries are integers from 0 to 99.</li> <li>b. In the Back Inservice field, enter the percentage of real servers in the primary server farm that must be active again for the ACE to place the server farm back into service. Valid entries are integers from 0 to 99. The value in this field should be larger than the value in the Partial Threshold Percentage field.</li> </ul> </li> <li>• <b>Redirect</b>—A server farm that consists only of real servers that redirect client requests to alternate locations specified in the real server configuration.</li> </ul> |
| Fail Action | <p>Select the action the ACE appliance is to take with respect to connections if any real server in the server farm fails:</p> <ul style="list-style-type: none"> <li>• <b>N/A</b>—Indicates that the ACE appliance is to take no action if any server in the server farm fails.</li> <li>• <b>Purge</b>—Indicates that the ACE appliance is to remove connections to a real server if that real server in the server farm fails. The ACE appliance sends a reset command to both the client and the server that failed.</li> <li>• <b>Reassign</b>—Indicates that the ACE reassign the existing server connections to the backup real server (if configured) if the real server fails after you enter this command. If a backup real server has not been configured for the failing server, this selection leaves the existing connections untouched in the failing real server.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 5-11 New Server Farm Attributes (continued)

| Field                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failaction<br>Reassign<br>Across Vlans | <p>This field appears only when the L7 Load-Balancing Action parameters are set as follows: Primary Action: LoadBalance, ServerFarm: New, Fail Action: Reassign.</p> <p>Check the check box to specify that the ACE reassigns the existing server connections to the backup real server on a different VLAN interface (commonly referred to as a bypass VLAN) if the real server fails. If a backup real server has not been configured for the failing server, this option has no effect and leaves the existing connections untouched in the failing real server.</p> <p>Note the following configuration requirements and restrictions when you enable this option:</p> <ul style="list-style-type: none"> <li>• Enable the Transparent option (see the next Field) to instruct the ACE not to use NAT to translate the ACE VIP address to the server IP address. The Failaction Reassign Across Vlans option is intended for use in stateful firewall load balancing (FWLB) on your ACE, where the destination IP address for the connection coming in to the ACE is for the end-point real server, and the ACE reassigns the connection so that it is transmitted through a different next hop.</li> <li>• Enable the MAC Sticky option on all server-side interfaces to ensure that packets that are going to and coming from the same server in a flow will traverse the same firewalls or stateful devices (see the <a href="#">“Configuring Virtual Context VLAN Interfaces”</a> section on page 10-10).</li> <li>• Configure the Predictor Hash Address option. See <a href="#">Table 5-12</a> for the supported predictor methods and configurable attributes for each predictor method.</li> <li>• You must configure identical policies on the primary interface and the backup-server interface. The backup interface must have the same feature configurations as the primary interface.</li> <li>• If you configure a policy on the backup-server interface that is different from the policies on the primary-server interface, that policy will be effective only for new connections. The reassigned connection will always have only the primary-server interface policies.</li> <li>• Interface-specific features (for example, NAT, application protocol inspection, outbound ACLs, or SYN cookie) are not supported.</li> <li>• You cannot reassign connections to the failed real server after it comes back up. This restriction also applies to same-VLAN backup servers.</li> <li>• Real servers must be directly connected to the ACE. This requirement also applies to same-VLAN backup server.</li> <li>• You must disable sequence number randomization on the firewall (see the <a href="#">“Configuring Connection Parameter Maps”</a> section on page 8-5).</li> <li>• Probe configurations should be similar on both ACEs and the interval values should be low. For example, if you configure a high interval value on ACE-1 and a low interval value on ACE-2, the reassigned connections may become stuck because of the probe configuration mismatch. ACE-2 with the low interval value will detect the primary server failure first and will reassign all its incoming connections to the backup-server interface VLAN. ACE-1 with the high interval value may not detect the failure before the primary server comes back up and will still point to the primary server.</li> </ul> <p>To minimize packet loss, we recommend the following probe parameter values on both ACEs: Interval: 2, Faildetect: 2, Passdetect interval: 2, and Passdetect count: 5.</p> |

Table 5-11 New Server Farm Attributes (continued)

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transparent              | <p>This field appears only for real servers identified as host servers.</p> <p>Check the check box to specify that network address translation from the VIP address to the server IP is to occur. Clear the check box to indicate that network address translation from the VIP address to the server IP address is not to occur (default).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Dynamic Workload Scaling | <p>This field appears only for host server farms.</p> <p>Allows the ACE to burst traffic to remote VMs when the average CPU usage, memory usage, or both of the local VMs has reached its specified maximum threshold value. The ACE stops bursting traffic to the remote VMs when the average CPU or memory usage of the local VMs has dropped to its specified minimum threshold value. This option requires that you have the ACE configured for Dynamic Workload Scaling using a Nexus 7000, VM Controller, and VM probe (see the <a href="#">“Configuring Dynamic Workload Scaling” section on page 6-14</a>).</p> <p>Click one of the following radio button options:</p> <ul style="list-style-type: none"> <li>N/A—Not applicable (default).</li> <li>Local—The ACE can use the VM Controller local VMs only for load balancing (bursting is not allowed).</li> <li>Burst—Enables the ACE to burst traffic to a remote VM Controller VMs.</li> </ul> <p>When you choose Burst, the VM Probe Name field appears along with a list of available VM probes. Choose an available VM probe or click <b>Add</b> to display the Health Monitoring pop-up window and create a new VM probe or edit an existing one (see the <a href="#">“Configuring Health Monitoring” section on page 6-39</a>).</p> |
| Fail-On-All              | <p>This field appears only for host server farms.</p> <p>By default, real servers that you configure in a server farm inherit the probes that you configure directly on that server farm. When you configure multiple probes on a server farm, the real servers in the server farm use an OR logic with respect to the probes, which means that if one of the probes configured on the server farm fails, all the real servers in that server farm fail and enter the PROBE-FAILED state.</p> <p>With AND logic, if one server farm probe fails, the real servers in the server farm remain in the OPERATIONAL state. If all the probes associated with the server farm fail, then all the real servers in that server farm fail and enter the PROBE-FAILED state. You can also configure AND logic for probes that you configure directly on real servers in a server farm.</p> <p>Check this check box to configure the real servers in a server farm to use AND logic with respect to multiple server farm probes.</p> <p>The Fail On All function is applicable to all probe types.</p>                                                                                                                                                                                                            |

Table 5-11 New Server Farm Attributes (continued)

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inband-Health Check                | <p>This field appears only for host server farms.</p> <p>By default, the ACE monitors the health of all real servers in a configuration through the use of ARPs and health probes. However, there is latency period between when the real server goes down and when the ACE becomes aware of the state. The inband health monitoring feature allows the ACE to monitor the health of the real servers in the server farm through the following connection failures:</p> <ul style="list-style-type: none"> <li>For TCP, resets (RSTs) from the server or SYN timeouts.</li> <li>For UDP, ICMP Host, Network, Port, Protocol, and Source Route unreachable messages.</li> </ul> <p>When you configure the failure-count threshold and the number of these failures exceeds the threshold within the reset-time interval, the ACE immediately marks the server as failed, takes it out of service, and removes it from load balancing. The server is not considered for load balancing until the optional resume-service interval expires.</p> <p>Choose one of the following:</p> <ul style="list-style-type: none"> <li>Count—Tracks the total number of TCP or UDP failures, and increments the counters as displayed by the <b>show serverfarm name inband</b> CLI command.</li> <li>Log—Logs a syslog error message when the number of events reaches the configured connection failure threshold.</li> <li>Remove—Logs a syslog error message when the number of events reaches the threshold and removes the server from service.</li> </ul> <p><b>Note</b> You can configure this feature and health probes to monitor a server. When you do, both are required to keep a real server in service within a server farm. If either feature detects a server is out of service, the ACE does not select the server for load balancing.</p> |
| Connection Failure Threshold Count | <p>This field appears only when the Inband-Health Check is set to Log or Remove.</p> <p>Enter the maximum number of connection failures that a real server can exhibit in the reset-time interval before ACE marks the real server as failed. Valid entries are integers from 1 to 4294967295.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Reset Timeout (Milliseconds)       | <p>This field appears only when the Inband-Health Check is set to Log or Remove.</p> <p>Enter the number of milliseconds for the reset-time interval. Valid entries are integers from 100 to 300000. The default interval is 100.</p> <p>This interval starts when the ACE detects a connection failure. If the connection failure threshold is reached during this interval, the ACE generates a syslog message. When the Inband-Health Check is set to Remove, the ACE also removes the real server from service.</p> <p>Changing the setting of this option affects the behavior of the real server, as follows:</p> <ul style="list-style-type: none"> <li>When the real server is in the OPERATIONAL state, even if several connection failures have occurred, the new reset-time interval takes effect the next time that a connection error occurs.</li> <li>When the real server in the INBAND-HM-FAILED state, the new reset-time interval takes effect the next time that a connection error occurs after the server transitions to the OPERATIONAL state.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



Table 5-11 New Server Farm Attributes (continued)

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resume Service (Seconds) | <p>This field appears only when the Inband-Health Check is set to Remove.</p> <p>Enter the number of seconds after a server has been marked as failed to reconsider it for sending live connections. Valid entries are integers from 30 to 3600. The default setting is 0. The setting of this option affects the behavior of the real server in the inband failed state, as follows:</p> <ul style="list-style-type: none"> <li>When this field is not configured and has the default setting of 0, the real server remains in the failed state until you manually suspend and then reactivate it.</li> <li>When this field is not configured and has the default setting of 0 and then you configure this option with an integer between 30 and 3,600, the failed real server immediately transitions to the Operational state.</li> <li>When you configure this field and then increase the value, the real server remains in the failed state for the duration of the previously-configured value. The new value takes effect the next time the real server transitions to the failed state.</li> <li>When you configure this field and then decrease the value, the failed real server immediately transitions to the Operational state.</li> <li>When you configure this field with an integer between 30 and 3,600 and then reset it to the default of 0, the real server remains in the failed state for the duration of the previously-configured value. The default setting takes effect the next time the real server transitions to the failed state. Then the real server remains in the failed state until you manually suspend and then reactivate it.</li> <li>When you change this field within the reset-time interval and the real server is in the OPERATIONAL state with several connection failures, the new threshold interval takes effect the next time that a connection error occurs, even if it occurs within the current reset-time interval.</li> </ul> |
| Predictor                | <p>Specify the method for selecting the next server in the server farm to respond to client requests. Round Robin is the default predictor method for a server farm.</p> <p>See <a href="#">Table 5-12</a> for the supported predictor methods and configurable attributes for each predictor method.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 5-11 New Server Farm Attributes (continued)



| Field  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Probes | <p>Specify the health monitoring probes to use:</p> <ul style="list-style-type: none"> <li>To include a probe that you want to use for health monitoring, select it in the Available list, and then click <b>Add</b>. The probe appears in the Selected list.</li> </ul> <p>The redirect real server probe list contains only configured probes of the type Is Routed, which means that the ACE routes the probe address according to the ACE internal routing table (see the <a href="#">“Configuring Health Monitoring for Real Servers”</a> section on page 6-41).</p> <p> <b>Note</b> You can associate both IPv6 and IPv4 probes to a server farm.</p> <p> <b>Note</b> The list of available probes does not include VM health monitoring probes. To choose a VM probe for monitoring local VM usage, see the <a href="#">Dynamic Workload Scaling</a> field.</p> <ul style="list-style-type: none"> <li>To remove a probe that you do not want to use for health monitoring, select it in the Selected list, and then click <b>Remove</b>. The probe appears in the Available list.</li> <li>To specify a sequence for probe use, select probes in the Selected list, and then click <b>Up</b> or <b>Down</b> until you have the desired sequence.</li> <li>To view the configuration for an existing probe, select a probe in the list on the right, and then click <b>View</b>.</li> <li>To display statistics and status information for an existing probe, choose a probe in the list on the right, and click <b>Details</b>. DM accesses the <b>show probe name detail</b> CLI command to display detailed probe information. See the <a href="#">“Displaying Health Monitoring Statistics and Status Information”</a> section on page 6-69.</li> </ul> <p>To add a new probe, click <b>Create</b>. See the <a href="#">“Configuring Health Monitoring for Real Servers”</a> section on page 6-41 for details on adding a new health monitoring probe and defining attributes for the specific probe type. In addition, set the following probe configuration parameters in the Probes section under Server Farm:</p> <ul style="list-style-type: none"> <li>Expect Addresses—To configure expect addresses for a DNS probe in Expect Addresses configuration screen, in the IPv4/IPv6 Address field, enter the IP address that the ACE appliance expects as a server response to a DNS request. You can enter multiple addresses in this field. However, you cannot mix IPv4 and IPv6 addresses.</li> <li>Probe Headers—To configure probe headers for either an HTTP or HTTPS probe, in the Probe Headers field enter the name of the HTTP header and the value to be matched using the format <code>header_name=header_value</code> where: <ul style="list-style-type: none"> <li><code>header_name</code> represents the HTTP header name the probe is to use. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.</li> <li><code>header_value</code> represents the string to assign to the header field. Valid entries are text strings with a maximum of 255 characters. If the string includes spaces, enclose the string with quotes.</li> </ul> </li> </ul> |

Table 5-11 New Server Farm Attributes (continued)

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Probes (Cont.) | <ul style="list-style-type: none"> <li>Probe Expect Status—To configure probe expect status for an FTP, HTTP, HTTPS, RTSP, SIP-TCP, SIP-UDP, or SMTP probe, in the Probe Expect Status field enter the following information: <ul style="list-style-type: none"> <li>To configure a single expect status code, enter the minimum expect status code for this probe followed by the same expect status code that you entered as the minimum. Valid entries are integers from 0 to 999.</li> <li>To configure a range of expect status codes, enter the lower limit of the range of status codes followed by the upper limit of the range of status codes. The maximum expect status code must be greater than or equal to the value specified for the minimum expect status code. Valid entries are integers from 0 to 999.</li> </ul> </li> <li>SNMP OID Table—To configure the SNMP OID for an SNMP probe, see the <a href="#">“Configuring an OID for SNMP Probes”</a> section on page 6-68.</li> </ul> <p>After you add a probe, you can modify the attributes for a health probe from the Health Monitoring table (<b>Config &gt; Virtual Contexts &gt; context &gt; Load Balancing &gt; Health Monitoring</b>) as described in the <a href="#">“Configuring Health Monitoring for Real Servers”</a> section on page 6-41. You can also delete an existing health probe from the Health Monitoring table.</p> |

Table 5-11 New Server Farm Attributes (continued)

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Real Servers | <p>The Real Servers table allows you to add, modify, remove, or change the order of real servers.</p> <ol style="list-style-type: none"> <li>1. Select an existing server, or click <b>Add</b> to add a real server to the server farm: <ul style="list-style-type: none"> <li>– If you select an existing server, you can view, modify, or duplicate the server's existing configuration. See the <a href="#">“Shared Objects and Virtual Servers”</a> section on page 5-9 for more information about modifying shared objects.</li> <li>– If you click <b>Add</b>, the table refreshes and allows you to enter server information.</li> </ul> </li> <li>2. For the IP Address Type, select either IPv6 or IPv4.</li> <li>3. In the IP Address field, enter the IP address.</li> <li>4. In the Name field, enter the name of the real server.</li> <li>5. In the Port field, enter the port number to be used for server port address translation (PAT). Valid entries are integers from 1 to 65535.</li> <li>6. In the Weight field, enter the weight to assign to this server in the server farm. Valid entries are integers from 1 to 100, and the default is 8.</li> <li>7. In the Redirection Code field, select the appropriate redirection code. This field appears only for real servers identified as redirect servers. <ul style="list-style-type: none"> <li>– N/A—Indicates that the webhost redirection code is not defined.</li> <li>– 301—Indicates that the requested resource has been moved permanently. For future references to this resource, the client should use one of the returned URIs.</li> <li>– 302—Indicates that the requested resource has been found, but has been moved temporarily to another location. For future references to this resource, the client should use the request URI because the resource may be moved to other locations from time to time.</li> </ul> </li> <li>8. In the Web Host Redirection field, enter the URL string used to redirect requests to another server. This field appears only for real servers identified as redirect servers. Enter the URL and port used to redirect requests to another server. Valid entries are in the form <code>http://host.com:port</code> where host is the name of the server and port is the port to be used. Valid host entries are unquoted text strings with no spaces and a maximum of 255 characters. Valid port numbers are from 1 to 65535. <p>The relocation string supports the following special characters:</p> <ul style="list-style-type: none"> <li>– %h—Inserts the hostname from the request Host header</li> <li>– %p—Inserts the URL path string from the request</li> </ul> </li> <li>9. In the Rate Bandwidth, field, specify the real server bandwidth limit in bytes per second. Valid entries are integers from 1 to 300000000.</li> <li>10. In the Rate Connection field, specify the limit for connections per second. Valid entries are integers from 1 to 350000.</li> <li>11. In the State field, select the administrative state of this server: <ul style="list-style-type: none"> <li>– In Service—The server is to be placed in use as a destination for server load balancing</li> <li>– In Service Standby—The server is a backup server and is to remain inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.</li> <li>– Out Of Service—The server is not to be placed in use by a server load balancer as a destination for client connections.</li> </ul> </li> </ol> |

Table 5-11 New Server Farm Attributes (continued)

| Field                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Real Servers<br>(continued) | <p>12. In the Buddy Real Group field, associate the real server with a buddy group by creating a buddy real server group or select an existing one (for more information, see the <a href="#">“Buddy Sticky Groups”</a> section on page 7-6).</p> <p>13. In the Fail-On-All field, check this check box to configure a real server to remain in the OPERATIONAL state unless all probes associated with it fail (AND logic). The Fail-On-All function is applicable to all probe types.</p> <p>Fail-On-All is applicable only for host real servers.</p> <p>14. In the Cookie String field, enter a cookie string value of the real server, which is to be used for HTTP cookie insertion when establishing a sticky connection. Valid entries are text strings with a maximum of 32 alphanumeric characters. You can include spaces and special characters in a cookie string value. See <a href="#">Chapter 7, “Configuring Stickiness”</a> for details on HTTP cookie sticky connections.</p> <p>Cookie String is applicable only for host real servers</p> <p>15. Do the following:</p> <ul style="list-style-type: none"> <li>– Click <b>OK</b> to accept your entries and add this real server to the server farm. The table refreshes with updated information.</li> <li>– Click <b>Cancel</b> to exit this procedure without saving your entries and to return to the Real Servers table.</li> </ul> <p>To display statistics and status information for an existing real server, choose a real server in the list, and then click <b>Details</b>. DM accesses the <b>show rserver name detail</b> CLI command to display detailed real server information. See the <a href="#">“Displaying Real Server Statistics and Status Information”</a> section on page 6-8.</p> |

Table 5-12 Predictor Methods and Attributes

| Predictor Method | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash Address     | <p>The ACE selects the server using a hash value based on the source or destination IP address.</p> <p>To configure the hash address predictor method:</p> <ol style="list-style-type: none"> <li>In the Mask Type field, indicate whether server selection is based on the source IP address or the destination IP address: <ul style="list-style-type: none"> <li>N/A—Indicates that this option is not defined.</li> <li>Destination—Indicates that the server is selected based on the destination IP address.</li> <li>Source—Indicates that the server is selected based on the source IP address.</li> </ul> </li> <li>In the IP Netmask field, select the subnet mask to apply to the address. If none is specified, the default is 255.255.255.255.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Hash Content     | <p>The ACE selects the server by using a hash value based on the specified content string of the HTTP packet body.</p> <ol style="list-style-type: none"> <li>In the Begin Pattern field, enter the beginning pattern of the content string and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the Length field, enter the length in bytes of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. <p>The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.</p> <p>You cannot specify both the length and the end-pattern options for a Hash Content predictor.</p> </li> <li>In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.</li> </ol> |
| Hash Cookie      | <p>The ACE selects the server by using a hash value based on the cookie name.</p> <p>In the Cookie Name field, enter a cookie name in the form of an unquoted text string with no spaces and a maximum of 64 characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Table 5-12 Predictor Methods and Attributes (continued)

| Predictor Method      | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash Secondary Cookie | <p>The ACE selects the server by using the hash value based on the specified cookie name in the URL query string, not the cookie header.</p> <p>In the Cookie Name field, enter a cookie name in the form of an unquoted text string with no spaces and a maximum of 64 characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Hash Header           | <p>The ACE selects the server by using a hash value based on the header name.</p> <p>In the Header Name field, select the HTTP header to be used for server selection:</p> <ul style="list-style-type: none"> <li>To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button and enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</li> <li>To specify one of the standard HTTP headers, select the second radio button, and then select one of the HTTP headers from the list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Hash Layer 4          | <p>The ACE selects the server by using a Layer 4 generic protocol load-balancing method. Use this predictor to load balance packets from protocols that are not explicitly supported by the ACE.</p> <ol style="list-style-type: none"> <li>In the Begin Pattern field, enter the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</li> </ol> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> <ol style="list-style-type: none"> <li>In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</li> </ol> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> <ol style="list-style-type: none"> <li>In the Length field, enter the length in bytes of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes.</li> </ol> <p>The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.</p> <p>You cannot specify both the length and end-pattern options for a Hash Layer 4 predictor.</p> <ol style="list-style-type: none"> <li>In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.</li> </ol> |

Table 5-12 Predictor Methods and Attributes (continued)

| Predictor Method  | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash URL          | <p>The ACE selects the server by using a hash value based on the URL. Use this method to load balance firewalls.</p> <p>Enter values in one or both of the pattern fields:</p> <ul style="list-style-type: none"> <li>In the URL Begin Pattern field, enter the beginning pattern of the URL and the pattern string to parse.</li> <li>In the URL End Pattern field, enter the ending pattern of the URL and the pattern string to parse.</li> </ul> <p>Valid entries for these fields are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters for each pattern you configure.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Least Bandwidth   | <p>The ACE selects the server with the least amount of network traffic over a specified sampling period.</p> <ol style="list-style-type: none"> <li>In the Assess Time field, enter the number of seconds for which the ACE is to collect traffic information. Valid entries are integers from 1 to 10 seconds.</li> <li>In the Least Bandwidth Samples field, enter the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Least Connections | <p>The ACE selects the server with the fewest number of connections.</p> <p>In the Slowstart Duration field, enter the slow-start value to be applied to this predictor method. Valid entries are integers from 1 to 65535, where 1 is the slowest ramp-up value.</p> <p>The slow-start mechanism is used to avoid sending a high rate of new connections to servers that you have just put into service.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Least Loaded      | <p>The ACE selects the server with the lowest load based on information from SNMP probes.</p> <ol style="list-style-type: none"> <li>In the SNMP Probe Name field, select the name of the SNMP probe to use.</li> <li>In the Auto Adjust field, configure the autoadjust feature to instruct the ACE to apply the maximum load of 16000 to a real server whose load reaches zero or override the default behavior. By default, the ACE applies the average load of the server farm to a real server whose load is zero. The ACE periodically adjusts this load value based on feedback from the server's SNMP probe and other configured options.</li> </ol> <p>Options are as follows:</p> <ul style="list-style-type: none"> <li>Average—Applies the average load of the server farm to a real server whose load is zero. This setting allows the server to participate in load balancing, while preventing it from being flooded by new connections. This is the default setting.</li> <li>Maxload—Instruct the ACE to apply the maximum load of 16000 to a real server whose load reaches zero.</li> <li>Off—Instruct the ACE to send all new connections to the server that has a load of zero until the next load update arrives from the SNMP probe for this server. If two servers have the same lowest load (either zero or nonzero), the ACE load balances the connections between the two servers in a round-robin manner.</li> </ul> <ol style="list-style-type: none"> <li>In the Weight Connection field, check the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.</li> </ol> |



Table 5-12 Predictor Methods and Attributes (continued)

| Predictor Method | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Response         | <p>The ACE selects the server with the lowest response time for a requested response-time measurement.</p> <ol style="list-style-type: none"> <li>In the Response Type field, select the type of measurement to use: <ul style="list-style-type: none"> <li>App-Req-To-Resp—The response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.</li> <li>Syn-To-Close—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server.</li> <li>Syn-To-Synack—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a SYN-ACK from the server.</li> </ul> </li> <li>In the Response Samples field, enter the number of samples over which you want to average the results of the response-time measurement. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).</li> <li>In the Weight Connection field, check the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.</li> </ol> |
| Round Robin      | The ACE selects the next server in the list of servers based on server weight. This is the default predictor method.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table 5-13 Sticky Group Attributes

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name  | Enter a unique identifier for the sticky type. You can either accept the automatically incremented entry given or you can enter your own. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Type        | <p>Select the method to be used when establishing sticky connections:</p> <ul style="list-style-type: none"> <li>• HTTP Content—The virtual server is to stick client connections to the same real server based on a string in the data portion of the HTTP packet. See <a href="#">Table 7-2</a> for additional configuration options.</li> <li>• HTTP Cookie—Indicates that the virtual server is either to learn a cookie from the HTTP header of a client request or to insert a cookie in the Set-Cookie header of the response from the server to the client, and then use the learned cookie to provide stickiness between the client and server for the duration of the transaction.</li> <li>• HTTP Header—Indicates that the virtual server is to stick client connections to the same real server based on HTTP headers.</li> <li>• IP Netmask—Indicates that the virtual server is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IPv4 address, the destination IPv4 address, or both.</li> </ul> <p><b>Note</b> If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence.</p> <ul style="list-style-type: none"> <li>• V6 Prefix—Indicates that the virtual server is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IPv6 address, the destination IPv6 address, or both.</li> <li>• Layer 4 Payload—The virtual server is to stick client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. See <a href="#">Table 7-6</a> for additional configuration options.</li> <li>• RADIUS—The virtual server is to stick client connections to the same real server based on a RADIUS attribute. See <a href="#">Table 7-7</a> for additional configuration options.</li> <li>• RTSP Header—The virtual server is to stick client connections to the same real server based on the RTSP Session header field. <a href="#">Table 7-8</a> for additional configuration options.</li> <li>• SIP Header—The virtual server is to stick client connections to the same real server based on the SIP Call-ID header field.</li> </ul> |
| Cookie Name | <p>This option appears for sticky type HTTP Cookie.</p> <p>Enter a unique identifier for the cookie. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 5-13 Sticky Group Attributes (continued)

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Insert      | <p>This option appears for sticky type HTTP Cookie.</p> <p>Check this check box if the virtual server is to insert a cookie in the Set-Cookie header of the response from the server to the client. This option is useful when you want to use a session cookie for persistence but the server is not currently setting the appropriate cookie. When selected, the virtual server selects a cookie value that identifies the original server from which the client received a response. For subsequent connections of the same transaction, the client uses the cookie to stick to the same server.</p> <p>Clear this check box to disable cookie insertion.</p> |
| Browser Expire     | <p>This option appears for sticky type HTTP Cookie and you select Enable Insert.</p> <p>Check this check box to allow the client's browser to expire a cookie when the session ends.</p> <p>Clear this check box to disable browser expire.</p>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Offset (Bytes)     | <p>This option appears for sticky types HTTP Cookie and HTTP Header.</p> <p>Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.</p>                                                                                                                                                                                                                                                                                                                     |
| Length (Bytes)     | <p>This option appears for sticky types HTTP Cookie and HTTP Header.</p> <p>Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE appliance is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.</p>                                                                                                                                                                                                                                                                                                                                                                 |
| Secondary Name     | <p>This option appears for sticky type HTTP Cookie.</p> <p>Enter an alternate cookie name that is to appear in the URL string of the Web page on the server. The virtual server uses this cookie to maintain a sticky connection between a client and a server and adds a secondary entry in the sticky table. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</p>                                                                                                                                                                                                                                                        |
| Header Name        | <p>This option appears for sticky type HTTP Header.</p> <p>Select the HTTP header to use for sticking client connections.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Netmask            | <p>This field appears for sticky type IP Netmask. This field is optional for the sticky type V6 Prefix.</p> <p>Select the netmask to apply to the source IPv4 address, destination IPv4 address, or both.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Prefix Length      | <p>This field appears for sticky type V6 Prefix. This field is optional for the sticky type IP Netmask.</p> <p>Enter the prefix length to apply to the source IPv6 address, destination IPv6 address, or both.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Address Type       | <p>This field appears for sticky type IP Netmask.</p> <p>Indicate whether this sticky type is to be applied to the client source IP address, the destination IP address, or both:</p> <ul style="list-style-type: none"> <li>Both—Indicates that this sticky type is to be applied to both the source IP address and the destination IP address.</li> <li>Destination—Indicates that this sticky type is to be applied to the destination IP address only.</li> <li>Source—Indicates that this sticky type is to be applied to the source IP address only.</li> </ul>                                                                                            |
| Sticky Server Farm | <p>Select an existing server farm to act as the primary server farm for this sticky group, or select <b>*New*</b> to create a new server farm. If you select <b>*New*</b>, configure the server farm using the information in <a href="#">Table 5-11</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                    |

Table 5-13 Sticky Group Attributes (continued)

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup Server Farm                  | Select an existing server farm to act as the backup server farm this sticky group, or select <b>*New*</b> to create a new server farm. If you select <b>*New*</b> , configure the server farm using the information in <a href="#">Table 5-11</a> .                                                                                                                                                                                                                                                                           |
| Aggregate State                     | <p>Check this check box to indicate that the state of the primary server farm is to be tied to the state of all real servers in the server farm and in the backup server farm, if configured. The ACE appliance declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.</p> <p>Clear this check box if the state of the primary server farm is not to be tied to all real servers in the server farm and in the backup server farm.</p> |
| Enable Sticky On Backup Server Farm | Check this check box to specify that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky.                                                                                                                                                                                                                                                                                                                                                                                          |
| Buddy Group                         | Associate the serverfarm with a buddy member group by creating a buddy sticky group or selecting an existing one (for more information, see the <a href="#">“Buddy Sticky Groups” section on page 7-6</a> ).                                                                                                                                                                                                                                                                                                                  |
| Replicate On HA Peer                | <p>Check this check box to indicate that the virtual server is to replicate sticky table entries on the backup server farm. If a failover occurs and this option is selected, the new active server farm can maintain the existing sticky connections.</p> <p>Clear this check box to indicate that the virtual server is not to replicate sticky table entries on the backup server farm.</p>                                                                                                                                |
| Timeout (Minutes)                   | Enter the number of minutes that the virtual server keeps the sticky information for a client connection in the sticky table after the latest client connection terminates. Valid entries are integers from 1 to 65535; the default is 1440 minutes (24 hours).                                                                                                                                                                                                                                                               |
| Timeout Active Connections          | <p>Check this check box to specify that the virtual server is to time out sticky table entries even if active connections exist after the sticky timer expires.</p> <p>Clear this check box to specify that the virtual is not to time out sticky table entries even if active connections exist after the sticky timer expires. This is the default behavior.</p>                                                                                                                                                            |

- Step 9** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the ACE compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.



**Note** By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Administration Guide, Cisco ACE Application Control Engine* for information on ACE licensing options.

Options are as follows:

- **Deflate**—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. deflate, the data format for compression described in RFC1951
- **Gzip**—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.

- N/A—HTTP compression is disabled.

When configuring HTTP compression, we recommend that you exclude the following MIME types from HTTP compression: “.gif”, “.css”, “.js”, “.class”, “.jar”, “.cab”, “.txt”, “.ps”, “.vbs”, “.xsl”, “.xml”, “.pdf”, “.swf”, “.jpg”, “.jpeg”, “.jpe”, or “.png”.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/\*).
- Minimum size—512 bytes.
- User agent—None.

**Step 10** In the SSL Initiation field, select an existing service, or select **\*New\*** to create a new service.



**Note** The SSL Initiation field appears only in the Advanced View, and when TCP is the selected protocol and Other, HTTP, or HTTPS is the application protocol.



**Note** The SSL initiation option does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

SSL initiation allows the virtual server to act as an SSL proxy client to initiate and maintain an SSL connection between itself and an SSL server. In this particular application, the ACE receives clear text from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the ACE decrypts the ciphertext that it receives from the SSL server and sends the data to the client as clear text.

- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See the [“Shared Objects and Virtual Servers”](#) section on page 5-9 for more information about modifying shared objects.
- If you select **\*New\***, configure the service using the information in [Table 5-14](#).

**Table 5-14** *Virtual Server SSL Initiation Attributes*

| Field           | Description                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | Enter a name for this SSL proxy service. Valid entries are alphanumeric strings with a maximum of 26 characters.                                                                                                                                                                                                               |
| Keys            | Select the SSL key pair to use during the SSL handshake for data encryption.                                                                                                                                                                                                                                                   |
| Certificates    | Select the SSL certificate to use during the SSL handshake.                                                                                                                                                                                                                                                                    |
| Chain Groups    | Select the chain group to use during the SSL handshake.                                                                                                                                                                                                                                                                        |
| Auth Groups     | Select the SSL authentication group to associate with this proxy server service.                                                                                                                                                                                                                                               |
| CRL Best-Effort | This option appears if you select an authentication group in the Auth Group Name field.<br><br>Check the check box to allow the ACE to search client certificates for the service to determine if it contains a CRL in the extension and retrieve the value, if it exists.<br><br>Clear the check box to disable this feature. |

Table 5-14 Virtual Server SSL Initiation Attributes

| Field          | Description                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| CRL Name       | This option appears if the CRL Best-Effort check box is clear.<br>Select the Certificate Revocation List if the ACE is to use for this proxy service. |
| Parameter Maps | Select the SSL parameter map to associate with this proxy server service.                                                                             |

For more information about SSL, see the “[Configuring SSL](#)” section on page 9-1.

**Step 11** In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format *header\_name=header\_value* where:

- *header\_name* represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
- *header\_value* represents the expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 12-33](#) lists the supported characters that you can use in regular expressions.

For example, you might enter `Host=www.cisco.com`.

**Step 12** Do the following:

- Click **OK** to save your entries and to return to the Rule Match table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule Match table.

**Step 13** If you are adding Rule Match entries for a new virtual server and you want to modify the sequence of rules in the L7 Load Balancing section of the Virtual Server configuration page, click **Up** or **Down** to change the order of the entries in the Rule Match table.



**Note** The Up and Down buttons are not available for an existing virtual server, only for a new virtual server. To reorder the entries in the Rule Match table for an existing virtual server, go to Config > Expert > Policy Maps and choose the Layer 7 load balancing policy map, delete the rule entry that you want to reorder, and then add it again by using the Insert Before option to put it in the correct order. See the “[Configuring Rules and Actions for Policy Maps](#)” section on page 12-36 for details.

**Step 14** When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.

#### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Configuring Virtual Server Properties, page 5-10](#)
- [Configuring Virtual Server SSL Termination, page 5-18](#)

- [Configuring Virtual Server Protocol Inspection, page 5-20](#)

## Configuring Virtual Server Default Layer 7 Load Balancing

Use this procedure configure default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions.

### Assumption

A virtual server has been configured. See the “[Configuring Virtual Servers](#)” section on page 5-2 for information on configuring a virtual server.

### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for default Layer 7 load balancing, and then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Default L7 Load-Balancing Action**. The Default L7 Load-Balancing Action configuration pane appears.
- Step 4** In the Primary Action field, indicate the default action the virtual server is to take in response to client requests for content when specified match conditions are not met:
- **Drop**—Indicates that client requests that do not meet specified match conditions are to be discarded. Continue with [Step 7](#).
  - **Forward**—Indicates that client requests that do not meet specified match conditions are to be forwarded without performing load balancing on the requests. Continue with [Step 7](#).
  - **Load Balance**—Indicates that client requests for content are to be directed to a server farm. If you select Load Balance, server farm, backup server farm, and sticky configuration options appear. Continue with [Step 5](#).
  - **Sticky**—Client requests for content are handled by a sticky group when match conditions are met. Continue with [Step 6](#).
- Step 5** If you select Load Balance as the primary action, you can configure load balancing using a server farm, a server farm/backup server farm pair, an existing sticky group, or a new sticky group.



**Note** If you select an existing object in any of these scenarios, you can view, modify, or duplicate the selected object's existing configuration. See the “[Shared Objects and Virtual Servers](#)” section on [page 5-9](#) for more information about modifying shared objects in virtual servers.

Configure load-balancing using the information in [Table 5-10](#).

- Step 6** (Optional) If you chose Sticky as the primary action, in the Sticky Group field, choose an existing sticky group or click **\*New\*** to add a new sticky group (see [Table 5-13](#)).



**Note** To display statistics and status information for an existing server farm, choose a server farm in the list, and then click **Details**. DM accesses the **show serverfarm name detail** CLI command to display detailed server farm information. See the “[Displaying Server Farm Statistics and Status Information](#)” section on [page 6-39](#).



**Note** If you chose an existing sticky group, you can view, modify, or duplicate the selected object's existing configuration. See the [“Shared Objects and Virtual Servers” section on page 5-9](#) for more information about modifying shared objects in virtual servers.

- Step 7** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the ACE compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.



**Note** By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Administration Guide, Cisco ACE Application Control Engine* for information on ACE licensing options.

Options are as follows:

- Deflate—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. deflate, the data format for compression described in RFC1951
- Gzip—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.
- N/A—HTTP compression is disabled.

When configuring HTTP compression, we recommend that you exclude the following MIME types from HTTP compression: “.gif”, “.css”, “.js”, “.class”, “.jar”, “.cab”, “.txt”, “.ps”, “.vbs”, “.xsl”, “.xml”, “.pdf”, “.swf”, “.jpg”, “.jpeg”, “.jpe”, or “.png”.



**Note** If you enable the Gzip or Deflate compression format, the DM GUI automatically inserts a L7 Load Balance Primary Action to exclude the MIME types listed above. However, if you disable HTTP compression later on, you will need to remove the auto-inserted Load Balance Primary Action.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/\*).
- Minimum size—512 bytes.
- User agent—None.

- Step 8** In the SSL Initiation field, select an existing service, or select **\*New\*** to create a new service.



**Note** The SSL Initiation field appears only in the Advanced View, and when TCP is the selected protocol and Other, HTTP, or HTTPS is the application protocol.



**Note**

The SSL initiation option does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

SSL initiation allows the virtual server to act as an SSL proxy client to initiate and maintain an SSL connection between itself and an SSL server. In this particular application, the ACE receives clear text from an HTTP client, and encrypts and transmits the data as ciphertext to the SSL server. On the reverse side, the ACE decrypts the ciphertext that it receives from the SSL server and sends the data to the client as clear text.

- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See the [“Shared Objects and Virtual Servers”](#) section on page 5-9 for more information about modifying shared objects.
- If you select **\*New\***, configure the service using the information in [Table 5-14](#).

For more information about SSL, see the [“Configuring SSL”](#) section on page 9-1.

**Step 9** In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format *header\_name=header\_value* where:

- *header\_name* represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
- *header\_value* represents the expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 12-33](#) lists the supported characters that you can use in regular expressions.

For example, you might enter `Host=www.cisco.com`.

**Step 10** When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

**Related Topics**

- [Configuring Virtual Server Properties, page 5-10](#)
- [Configuring Virtual Server SSL Termination, page 5-18](#)
- [Configuring Virtual Server Protocol Inspection, page 5-20](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 5-30](#)

## Configuring Application Acceleration and Optimization

The ACE appliance includes configuration options that allow you to accelerate enterprise applications, resulting in increased employee productivity, enhanced customer retention, and increased online revenues. The application acceleration functions of the ACE appliance apply several optimization technologies to accelerate Web application performance. The application acceleration functionality in

the ACE appliance enables enterprises to optimize network performance and improve access to critical business information. This capability accelerates the performance of Web applications, including customer relationship management (CRM), portals, and online collaboration by up to 10 times.

See the “[Configuring Application Acceleration and Optimization](#)” section on page 13-1 or the *Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance* for more information about application acceleration and optimization.

Use this procedure to configure acceleration and optimization on virtual servers.

#### Assumption

A virtual server has been configured. See the “[Configuring Virtual Servers](#)” section on page 5-2 for information on configuring a virtual server.

#### Consideration

Application acceleration and optimization is only supported in IPv4 to IPv4 server load-balancing configurations.

#### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
  - Step 2** Select the virtual server you want to configure for optimization, and then click **Edit**. The Virtual Server configuration screen appears.
  - Step 3** Click **Application Acceleration And Optimization**. The Application Acceleration And Optimization configuration pane appears.
  - Step 4** In the Configuration field, indicate the method you want to use to configure application acceleration and optimization:
    - EZ—Indicates that you want to use standard acceleration and optimization options. Continue with [Step 5](#).
    - Custom—Indicates that you want to associate specific match criteria, actions, and parameter maps for application acceleration and optimization for this virtual server. If you choose this option, continue with [Step 6](#).
  - Step 5** If you select EZ, the Latency Optimization (FlashForward) and Bandwidth Optimization (Delta) fields appear.
    - a. Check the Latency Optimization (FlashForward) check box to indicate that the ACE appliance is to use bandwidth reduction and download acceleration techniques to objects embedded within HTML pages. Clear this check box to indicate that the ACE appliance is not to employ these techniques to objects embedded within HTML pages. Latency optimization corresponds to FlashForward functionality. For more information about FlashForward functionality, see the “[Optimization Overview](#)” section on page 13-2.
    - b. Check the Bandwidth Optimization (Delta) check box to indicate that the ACE appliance is to dynamically update client browser caches with content differences, or deltas. Clear this check box to indicate that the ACE appliance is not to dynamically update client browser caches. Bandwidth optimization corresponds to action list Delta optimization. For more information about Delta optimization, see the “[Optimization Overview](#)” section on page 13-2 and the “[Configuring an HTTP Optimization Action List](#)” section on page 13-3.
    - c. Continue with [Step 11](#).

- Step 6** If you select Custom, the Actions configuration pane appears with a table listing match criteria and actions. Click **Add** to add an entry to this table, or select an existing entry, and then click **Edit** to modify it. The configuration subset refreshes with the available configuration options.
- Step 7** In the Apply Template field, select one of the configuration templates for the type of optimization you want to configure, or leave blank to configure optimization without a template:
- Bandwidth Optimization—Maximizes bandwidth for Web-based traffic.
  - Latency Optimization For Embedded Objects—Reduces the latency associated with embedded objects in Web-based traffic.
  - Latency Optimization For Embedded Images—Reduces the latency associated with embedded images in Web-based traffic.
  - Latency Optimization For Containers—Reduces the latency associated with Web containers.
- If you do not select a template and select **\*New\*** in the Rule Match and Actions fields, you are creating your own optimization rules and actions.
- Step 8** In the Rule Match field, select an existing class map or click **\*New\*** to specify new match criteria:
- If you select an existing class map, you can view, modify, or duplicate the existing configuration. See the “[Shared Objects and Virtual Servers](#)” section on page 5-9 for more information about modifying shared objects.
  - If you click **\*New\***, the screen refreshes with the default configuration settings for the template you selected. You can accept the default settings or modify them using the information in [Table 5-15](#).

**Table 5-15** Optimization Rule Match Configuration Options

| Field      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name       | Enter a unique name for this match criteria rule.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Matches    | Select the method to be used to evaluate multiple match statements when multiple match conditions exist: <ul style="list-style-type: none"> <li>• Any—A match exists if at least one of the match conditions is satisfied.</li> <li>• All—A match exists only if all match conditions are satisfied.</li> </ul>                                                                                                                                                   |
| Conditions | Click <b>Add</b> to add a new set of conditions or select an existing entry, and then click <b>Edit</b> to modify it: <ol style="list-style-type: none"> <li>1. In the Type field, select the match condition to be used, and then configure any condition-specific options using the information in <a href="#">Table 5-9</a>.</li> <li>2. Click <b>OK</b> to save your entries, or <b>Cancel</b> to exit this procedure without saving your entries.</li> </ol> |

- Step 9** In the Actions field, select an existing action list to use for optimization or click **\*New\*** to create a new action list.
- If you select an existing optimization action list, you can view, modify, or duplicate the existing configuration. See the “[Shared Objects and Virtual Servers](#)” section on page 5-9 for more information about modifying shared objects.
  - If you click **\*New\***, the screen refreshes with the default configuration settings for the template you selected. You can accept the default settings or modify them using the information in [Table 5-16](#).

Table 5-16 Optimization Action List Configuration Options

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action List Name | Enter a unique name for the optimization action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Enable Delta     | <p>Delta optimization dynamically updates client browser caches directly with content differences, or deltas, resulting in faster page downloads.</p> <p>Check this check box to enable delta optimization for the specified URLs.</p> <p>Clear this check box to disable delta optimization for the specified URLs.</p> <p><b>Note</b> The ACE restricts you from enabling delta optimization if you have previously specified either Cache Dynamic or Dynamic Entity Tag.</p>                                                                                                                                                                                                                                                                                                    |
| Enable AppScope  | <p>AppScope runs on the Management Console of the optional Cisco AVS 3180A Management Station and measures end-to-end application performance.</p> <p>Check this check box to enable AppScope performance monitoring for use with the ACE appliance.</p> <p>Clear this check box to disable AppScope performance monitoring for use with the ACE appliance.</p>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Flash Forward    | <p>The FlashForward feature reduces bandwidth usage and accelerates embedded object downloading by combining local object storage with dynamic renaming of embedded objects, thereby enforcing object freshness within the parent HTML page.</p> <p>Specify how the ACE appliance is to implement FlashForward:</p> <ul style="list-style-type: none"> <li>• N/A—Indicates that this feature is not enabled.</li> <li>• Flash Forward—Indicates that FlashForward is to be enabled for the specified URLs and that embedded objects are to be transformed.</li> <li>• Flash Forward Object—Indicates that FlashForward static caching is to be enabled for the objects that the corresponding URLs refer to, such as Cascading Style Sheets (CSS), JPEG, and GIF files.</li> </ul> |
| Cache Dynamic    | <p>Check this check box to enable Adaptive Dynamic Caching for the specified URLs even if the expiration settings in the response indicate that the content is dynamic. The expiration of cache objects is controlled by the cache expiration settings based on time or server load.</p> <p>Clear this check box to disable this feature.</p> <p><b>Note</b> The ACE restricts you from enabling Cache Dynamic if you have previously specified either Enable Delta or Dynamic Entity Tag.</p>                                                                                                                                                                                                                                                                                     |
| Cache Forward    | <p>Check this check box to enables the cache forward feature for the corresponding URLs. Cache forward allows the ACE to serve the object from its cache (static or dynamic) even when the object has expired if the maximum cache TTL time period has not yet expired (set by specifying the Cache Time-To-Live Duration (%): field in an Optimization parameter map). At the same time, the ACE sends an asynchronous request to the origin server to refresh its cache of the object.</p> <p>Clear this check box to disable this feature.</p>                                                                                                                                                                                                                                  |

Table 5-16 Optimization Action List Configuration Options (continued)

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic Entity Tag                | <p>This feature enables the acceleration of noncacheable embedded objects, which results in improved application response time. When enabled, this feature eliminates the need for users to download noncacheable objects on each request.</p> <p>Check this check box to indicate that the ACE appliance is to implement just-in-time object acceleration for noncacheable embedded objects.</p> <p>Clear this check box to disable this feature.</p> <p><b>Note</b> The ACE restricts you from enabling Dynamic Entity Tag if you have previously specified either Enable Delta or Cache Dynamic.</p> |
| Fine Tune Optimization Parameters | <p>Click this header to configure additional optimization attributes. When expanded, the configuration pane displays options specific to the type of optimization you are configuring and features that you enable.</p> <p>Refer to <a href="#">Table 8-5</a> for information about specific options that appear.</p>                                                                                                                                                                                                                                                                                   |

**Step 10** When you finish configuring match criteria and actions, do the following:

- Click **OK** to save your entries and to return to the Rule Match and Actions table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule Match and Actions table.

**Step 11** When you finish configuring virtual server properties, do the following:

- Click **Deploy Now** to save your entries. The ACE appliance validates the optimization action list configuration and deploys it on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.

#### Related Topics

- [Configuring Virtual Server Properties, page 5-10](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)
- [Configuring Traffic Policies for HTTP Optimization, page 13-6](#)
- [Configuring Virtual Server Protocol Inspection, page 5-20](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 5-30](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55](#)

## Configuring Virtual Server NAT

Use this procedure to configure Name Address Translation (NAT) for virtual servers.

#### Assumptions

- A virtual server has been configured. See the “[Configuring Virtual Servers](#)” section on page 5-2 for information on configuring a virtual server.

- A VLAN has been configured. See the [“Configuring Virtual Context VLAN Interfaces”](#) section on page 10-10 for information on configuring a VLAN interface.
- At least one NAT pool has been configured on a VLAN interface. See the [“Configuring VLAN Interface NAT Pools and Displaying NAT Utilization”](#) section on page 10-32 for information on configuring a NAT pool.

#### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for NAT, and then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **NAT**. The NAT table appears.
- Step 4** Click **Add** to add an entry, or select an existing entry, and then click **Edit** to modify it.
- Step 5** In the VLAN field, select the VLAN you want to use NAT. For more information about NAT, see the [“Configuring VLAN Interface NAT Pools and Displaying NAT Utilization”](#) section on page 10-32.
- Step 6** In the NAT Pool ID field, select the NAT pool that you want to associate with the selected VLAN.
- Step 7** Do the following:
- Click **OK** to save your entries and to return to the NAT table. The NAT table refreshes with the new entry.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the NAT table.
- Step 8** When you finish configuring virtual server properties, do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
- 

#### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Configuring Virtual Server Properties, page 5-10](#)
- [Configuring Virtual Server SSL Termination, page 5-18](#)
- [Configuring Virtual Server Protocol Inspection, page 5-20](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 5-30](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 5-55](#)

## Displaying Virtual Server Statistics and Status Information

You can display virtual server statistics and status information for a particular virtual server by using the **Details** button.

#### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Virtual Servers**.

The Virtual Servers table appears.

- Step 2** In the Virtual Servers table, choose a virtual server from the Virtual Servers table, and click **Details**. The **show service-policy** *policy\_name* **class-map** *class\_name* **detail** CLI command output appears. For details about the displayed fields, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.



**Note** This feature requires ACE software Version A3(2.1) or later. An error displays with earlier software versions.

- Step 3** (Optional) Click **Update Details** to refresh the window information.

- Step 4** Click **Close** to return to the Virtual Servers table.

#### Related Topics

- [Configuring Virtual Servers, page 5-2](#)
- [Managing Virtual Servers, page 5-63](#)
- [Viewing All Virtual Servers, page 5-65](#)

## Managing Virtual Servers

After you have created a virtual server the following options are available:

| Task                                              | Related Topics                                                |
|---------------------------------------------------|---------------------------------------------------------------|
| Modify a virtual server configuration             | <a href="#">Configuring Virtual Servers, page 5-2</a>         |
| List virtual servers by virtual context           | <a href="#">Viewing Virtual Servers by Context, page 5-63</a> |
| Activate a virtual server                         | <a href="#">Activating Virtual Servers, page 5-64</a>         |
| Suspend a virtual server                          | <a href="#">Suspending Virtual Servers, page 5-65</a>         |
| View all virtual servers and its configured state | <a href="#">Viewing All Virtual Servers, page 5-65</a>        |

## Viewing Virtual Servers by Context

Use this procedure to view all virtual servers associated with a virtual context.

#### Procedure

- Step 1** Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.
- Step 2** Select the context associated with the virtual servers you want to view, and then select **Load Balancing > Virtual Servers**. The Virtual Servers table appears with the following information:
- Virtual server name
  - Configured state, such as Inservice
  - Virtual IP address

- Port
  - Associated VLANs
  - Associated server farms
  - Virtual context name
- 

**Related Topics**

- [Configuring Virtual Servers, page 5-2](#)
- [Managing Virtual Servers, page 5-63](#)

## Displaying Virtual Server Statistics and Status Information

You can display virtual server statistics and status information for a particular virtual server by using the **Details** button. DM accesses the **show service-policy *policy\_name* detail** CLI command to display detailed virtual server information.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > *context* > Load Balancing > Virtual Servers**.  
The Virtual Servers table appears.
- Step 2** In the Virtual Servers table, choose a virtual server from the Virtual Servers table, and click **Details**.  
The **show service-policy *policy\_name* detail** CLI command output appears. For details on the displayed output fields, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.
- Step 3** Click **Update Details** to refresh the output for the **show service-policy *policy\_name* detail** CLI command.
- Step 4** Click **Close** to return to the Virtual Servers table.
- 

**Related Topics**

- [Configuring Virtual Servers, page 5-2](#)
- [Managing Virtual Servers, page 5-63](#)
- [Viewing All Virtual Servers, page 5-65](#)

## Activating Virtual Servers

Use this procedure to activate a virtual server.

**Procedure**

- 
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.



- Step 2** Select the server that you want to activate, and then click **Activate**. The server is activated and the screen refreshes with updated information in the Configured State column.
- 

**Related Topics**

- [Managing Virtual Servers, page 5-63](#)
- [Viewing All Virtual Servers, page 5-65](#)
- [Suspending Virtual Servers, page 5-65](#)

## Suspending Virtual Servers

Use this procedure to suspend a virtual server.

**Procedure**

- 
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to suspend, and then click **Suspend**. The Suspend Virtual Server screen appears.
- Step 3** In the Reason field, enter the reason for this action. You might enter a trouble ticket, an order ticket, or a user message.



**Caution** Do not enter a password in the Reason field.

---

- Step 4** Do the following:
- Click **Deploy Now** to deploy this configuration. The virtual server is taken out of service and the Device Manager returns to the Virtual Servers table. The screen refreshes with updated information in the Oper State column.
  - Click **Cancel** to exit this procedure without suspending the virtual server and to return to the Virtual Servers table.
- 


**Related Topics**

- [Managing Virtual Servers, page 5-63](#)
- [Viewing All Virtual Servers, page 5-65](#)
- [Activating Virtual Servers, page 5-64](#)

## Viewing All Virtual Servers

To view all virtual servers, choose **Config > Operations > Virtual Servers**. The Virtual Servers table appears with the following information for each server: [Table 5-17](#) describes the Virtual Servers table information.

Table 5-17 Virtual Server Table Fields

| Item                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                     | Server farm name sorted by virtual context.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Policy Map               | Associated policy map.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IP Address/Protocol/Port | Server farm IP address, protocol, and port number used for communications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Context                  | Virtual context associated with the server farm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Admin                    | Administrative state of the virtual server: Up or Down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Oper                     | Operational state of the virtual server: Up or Down.<br>To display detailed information about the virtual server in a popup window, click the linked state value in this column.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                          |  <b>Note</b> The display virtual server details feature requires ACE software Version A3(2.1) or later. An error displays with earlier software versions.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DWS                      | Operating state of Dynamic Workload Scaling for the virtual server, which can be: <ul style="list-style-type: none"> <li>• N/A—Not applicable; the server farms associated with the virtual server are not configured to use Dynamic Workload Scaling.</li> <li>• Local—At least one server farm associated the virtual server is configured to use Dynamic Workload Scaling, but the ACE is sending traffic to the VM Controller's local VMs only.</li> <li>• Expanded—At least one server farm associated the virtual server is configured to use Dynamic Workload Scaling and the ACE is sending traffic to the VM Controller's local and remote VMs.</li> </ul> |
| Conn                     | Number of active connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Stat Age                 | Time as of the loading of the page since the SNMP values were polled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Server farms             | Associated server farms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| VLANs                    | Associated VLANs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

You can activate or suspend virtual servers from this table and obtain additional information about the state of the virtual server.

#### Related Topics

- [Activating Virtual Servers, page 5-64](#)
- [Suspending Virtual Servers, page 5-65](#)



## CHAPTER 6

# Configuring Real Servers and Server Farms

This chapter provides an overview of server load balancing and procedures for configuring real servers and server farms for load balancing on an ACE appliance.



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

This chapter contains the following sections:

- [Server Load Balancing Overview, page 6-1](#)
- [Configuring Real Servers, page 6-5](#)
- [Managing Real Servers, page 6-9](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)
- [Configuring Server Farms, page 6-18](#)
- [Configuring Health Monitoring, page 6-39](#)
- [Configuring Secure KAL-AP, page 6-70](#)

## Server Load Balancing Overview

Server load balancing (SLB) is the process of deciding to which server a load-balancing device should send a client request for service. For example, a client request can consist of an HTTP GET for a Web page or an FTP GET to download a file. The job of the load balancer is to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Depending on the load-balancing algorithm or predictor that you configure, the ACE appliance performs a series of checks and calculations to determine the server that can best service each client request. The ACE appliance bases server selection on several factors, including the server with the fewest connections with respect to load, source or destination address, cookies, URLs, or HTTP headers.

The ACE Appliance Device Manager allows you to configure load balancing using:

- Virtual servers—See [Configuring Virtual Servers, page 5-2](#).
- Real servers—See [Configuring Real Servers, page 6-5](#).
- Dynamic Workload Scaling—See [Configuring Dynamic Workload Scaling, page 6-14](#).
- Server farms—See [Configuring Server Farms, page 6-18](#).
- Sticky groups—See [Configuring Sticky Groups, page 7-11](#).
- Parameter maps—See [Configuring Parameter Maps, page 8-1](#).

For information about SLB as configured and performed by the ACE appliance, see the following topics:

- [Configuring Virtual Servers, page 5-2](#)
- [Load-Balancing Predictors, page 6-2](#)
- [Real Servers, page 6-3](#)
- [Dynamic Workload Scaling Overview, page 6-4](#)
- [Server Farms, page 6-5](#)
- [Configuring Health Monitoring, page 6-39](#)
- [TCL Scripts, page 6-40](#)
- [Configuring Stickiness, page 7-1](#)

## Load-Balancing Predictors

The ACE appliance uses the following predictors to select the best server to satisfy a client request:

- Hash Address—Selects the server using a hash value based on either the source or destination IP address, or both. Use these predictors for firewall load balancing (FWLB).



### Note

FWLB allows you to scale firewall protection by distributing traffic across multiple firewalls on a per-connection basis. All packets belonging to a particular connection must go through the same firewall. The firewall then allows or denies transmission of individual packets across its interfaces. For more information about configuring FWLB on the ACE appliance, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

- Hash Content—Selects the server by using a hash value based on the specified content string of the HTTP packet body
- Hash Cookie—Selects the server using a hash value based on a cookie name.
- Hash Secondary Cookie—The ACE selects the server by using the hash value based on the specified cookie name in the URL query string, not the cookie header.
- Hash Header—Selects the server using a hash value based on the HTTP header name.
- Hash Layer4—Selects the server using a Layer 4 generic protocol load-balancing method.
- Hash URL—Selects the server using a hash value based on the requested URL. You can specify a beginning pattern and an ending pattern to match in the URL. Use this predictor method to load-balance cache servers. Cache servers perform better with the URL hash method because you can divide the contents of the caches evenly if the traffic is random enough. In a redundant

configuration, the cache servers continue to work even if the active ACE appliance switches over to the standby ACE appliance. For information about configuring redundancy, see [Configuring High Availability, page 11-1](#).

- **Least Bandwidth**—Selects the server with the least amount of network traffic or a specified sampling period. Use this type for server farms with heavy traffic, such as downloading video clips.
- **Least Connections**—Selects the server with the fewest number of active connections based on server weight. For the least connection predictor, you can configure a slow-start mechanism to avoid sending a high rate of new connections to servers that you have just put into service.
- **Least Loaded**—Selects the server with the lowest load as determined by information from SNMP probes.
- **Response**—Selects the server with the lowest response time for a specific response-time measurement.
- **Round Robin**—Selects the next server in the list of real servers based on server weight (weighted roundrobin). Servers with a higher weight value receive a higher percentage of the connections. This is the default predictor.

**Note**

The different hash predictor methods do not recognize the weight value that you configure for real servers. The ACE uses the weight that you assign to real servers only in the round-robin and least-connections predictor methods.

**Related Topic**

[Configuring Health Monitoring, page 6-39](#)

## Real Servers

To provide services to clients, you configure real servers on the ACE appliance. Real servers are dedicated physical servers or VMware virtual machines (VMs) that you configure in groups called server farms.

**Note**

VMs that you define as real servers are VMs that the ACE recognizes when configured for Dynamic Workload Scaling (see the [“Configuring Dynamic Workload Scaling” section on page 6-14](#)).

These servers provide client services such as HTTP or XML content, website hosting, FTP file uploads or downloads, redirection for web pages that have moved to another location, and so on. You identify real servers with names and characterize them with IP addresses, connection limits, and weight values. The ACE appliance also allows you to configure backup servers in case a server is taken out of service for any reason.

After you create and name a real server on the ACE appliance, you can configure several parameters, including connection limits, health probes, and weight. You can assign a weight to each real server based on its relative importance to other servers in the server farm. The ACE appliance uses the server weight value for the weighted round-robin and the least-connections load-balancing predictors. The load-balancing predictor algorithms (for example, round-robin, least connections, and so on) determine the servers to which the ACE appliance sends connection requests. For a listing and brief description of the load-balancing predictors, see [Load-Balancing Predictors, page 6-2](#).

The ACE appliance uses traffic classification maps (class maps) within policy maps to filter out interesting traffic and to apply specific actions to that traffic based on the SLB configuration. You use class maps to configure a virtual server address and definition.

If a primary real server fails, the ACE appliance takes that server out of service and no longer includes it in load-balancing decisions. If you configured a backup server for the real server that failed, the ACE appliance redirects the primary real server connections to the backup server. For information about configuring a backup server, see the [Configuring Virtual Server Layer 7 Load Balancing](#), page 5-30.

The ACE appliance can take a real server out of service for the following reasons:

- Probe failure
- ARP timeout
- Neighbor Discovery (ND) failure (IPv6 only)
- Retcode failure
- Reaching the maximum number of connections
- Specifying Out Of Service as the administrative state of a real server
- Specifying In Service Standby as the administrative state of a real server

The Out Of Service and In Service Standby selections both provide the graceful shutdown of a server.

#### Related Topics

- [Configuring Real Servers](#), page 6-5
- [Configuring Health Monitoring for Real Servers](#), page 6-41

## Dynamic Workload Scaling Overview

The ACE Dynamic Workload Scaling feature permits on-demand access to remote resources, such as VMs, that you own or lease from an Internet service provider or cloud service provider. This feature uses Cisco Nexus 7000 Series switches with Overlay Transport Virtualization (OTV) technology to create a Data Center Interconnect (DCI) on a Layer 2 link over an existing IP network between geographically distributed data centers. The local data center Nexus 7000 contains an OTV forwarding table that lists the MAC addresses of the Layer 2 extended virtual private network (VPN) and identifies the addresses as either local or remote.

When you configure the ACE to use this feature, the ACE uses an XML query to poll the Cisco Nexus 7000 Series Switch and obtain the OTV forwarding table information to determine the locality of the local or remote VMs. The ACE also uses a health monitor probe that it sends to the local VMware vCenter Server to monitor the load of the local VMs based on CPU usage, memory usage, or both. When the average CPU or memory usage of the local VMs reaches its configured maximum threshold value, the ACE bursts traffic to the remote VMs. The ACE stops bursting traffic to the remote VMs when the average CPU or memory usage of the local VMs drops below its configured minimum threshold value.

To use Dynamic Workload Scaling, you configure the ACE to connect to the Data Center Interconnect device (Cisco Nexus 7000 Series switch) and the VMware Controller associated with the local and remote VMs. You also configure the ACE with the probe type VM to monitor a server farm's local VM CPU and memory usage, which determines when the ACE bursts traffic to the remote VMs.

For more details on this feature, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

**Related Topic**

- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Server Farms

Typically, in data centers, servers are organized into related groups called *server farms*. Servers within server farms often contain identical content (referred to as mirrored content) so that if one server becomes inoperative, another server can take its place immediately. Also, having mirrored content allows several servers to share the load of increased demand during important local or international events, such as the Olympic Games. This phenomenon of a sudden large demand for content is called a *flash crowd*.

After you create and name a server farm, you can add existing real servers to it and configure other server farm parameters, such as the load-balancing predictor, server weight, backup server, health probe, and so on. For a listing and brief description of load-balancing predictors, see [Load-Balancing Predictors, page 6-2](#).

**Related Topic**

[Configuring Server Farms, page 6-18](#)

## Configuring Real Servers

Real servers are dedicated physical servers that are typically configured in groups called server farms. These servers provide services to clients, such as HTTP or XML content, streaming media (video or audio), TFTP or FTP services, and so on. When configuring real servers, you assign names to them and specify IP addresses, connection limits, and weight values.

The ACE appliance uses traffic classification maps (class maps) within policy maps to filter specified traffic and to apply specific actions to that traffic based on the load-balancing configuration. A load-balancing predictor algorithm (round-robin or least connections) determines the servers to which the ACE appliance sends connection requests. For information about configuring class maps, see [Configuring Virtual Context Class Maps, page 12-8](#).

Use this procedure to configure load balancing on real servers.

**Procedure**

- 
- |               |                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; Load Balancing &gt; Real Servers</b> . The Real Servers table appears.                                    |
| <b>Step 2</b> | Click <b>Add</b> to add a new real server, or select a real server you want to modify, and then click <b>Edit</b> . The Real Servers configuration screen appears. |
| <b>Step 3</b> | Configure the server using the information in <a href="#">Table 6-1</a> .                                                                                          |

Table 6-1 Real Server Attributes

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name              | Either accept the automatically incremented value in this field, or enter a unique name for this server. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.                                                                                                                                                                                                                                                                                                              |
| Type              | Select the type of server: <ul style="list-style-type: none"> <li>Host—Indicates that this is a typical real server that provides content and services to clients.</li> <li>Redirect—Indicates that this server is used to redirect traffic to a new location.</li> </ul>                                                                                                                                                                                                                                    |
| State             | Select the state of this real server: <ul style="list-style-type: none"> <li>In Service—The real server is in service.</li> <li>Out Of Service—The real server is out of service.</li> </ul>                                                                                                                                                                                                                                                                                                                 |
| Description       | Enter a brief description for this real server. Valid entries are unquoted alphanumeric text strings with no spaces and a maximum of 240 characters.                                                                                                                                                                                                                                                                                                                                                         |
| IP Address Type   | These selections appear for only real servers specified as hosts.<br>Select the IP address type of this real server: <ul style="list-style-type: none"> <li>IPv6—The real server has an IPv6 address.</li> <li>IPv4—The real server has an IPv4 address.</li> </ul>                                                                                                                                                                                                                                          |
| IPv6/IPv4 Address | This field appears for only real servers specified as hosts.<br>Enter a unique IP address as indicated by the IP Address Type field. The IP address cannot be of an existing virtual IP address (VIP), real server or interface in the context.                                                                                                                                                                                                                                                              |
| Fail-On-All       | This field appears only for real servers identified as host servers.<br>By default, real servers with multiple probes configured for them have an OR logic associated with them. This means that if one of the real server probes fails, the real server fails and enters the PROBE-FAILED state.<br>Click this check box to configure a real server to remain in the OPERATIONAL state unless all probes associated with it fail (AND logic).<br>The Fail-On-All function is applicable to all probe types. |
| Min. Connections  | Enter the minimum number of connections to be allowed on this server before the ACE appliance starts sending connections again after it has exceeded the Max. Connections limit. This value must be less than or equal to the Max. Connections value. By default, this value is equal to the Max. Connections value. Valid entries are integers from 1 to 4000000.                                                                                                                                           |
| Max. Connections  | Enter the maximum number of active connections allowed on this server. When the number of connections exceeds this value, the ACE appliance stops sending connections to this server until the number of connections falls below the Min. Connections value. Valid entries are integers from 1 to 4000000, and the default is 4000000.                                                                                                                                                                       |



Table 6-1 Real Server Attributes (continued)



| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Weight               | <p>This field appears only for real servers identified as hosts.</p> <p>Enter the weight to be assigned to this real server in a server farm. Valid entries are integers from 1 to 100, and the default is 8.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Web Host Redirection | <p>URL string used to redirect requests to another server. This field appears only for real servers identified as redirect servers. Enter the URL and port used to redirect requests to another server.</p> <p>Valid entries are in the form <code>http://host.com:port</code> where <i>host</i> is the name of the server and <i>port</i> is the port to be used. Valid host entries are unquoted text strings with no spaces and a maximum of 255 characters. Valid port numbers are from 1 to 65535.</p> <p>The relocation string supports the following special characters:</p> <ul style="list-style-type: none"> <li>• %h—Inserts the hostname from the request Host header</li> <li>• %p—Inserts the URL path string from the request</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Redirection Code     | <p>This field appears only for real servers identified as redirect servers.</p> <p>Select the appropriate redirection code:</p> <ul style="list-style-type: none"> <li>• N/A—Indicates that the webhost redirection code is not defined.</li> <li>• 301—Indicates that the requested resource has been moved permanently. For future references to this resource, the client should use one of the returned URIs.</li> <li>• 302—Indicates that the requested resource has been found, but has been moved temporarily to another location. For future references to this resource, the client should use the request URI because the resource may be moved to other locations from time to time.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Probes               | <p>In the Probes field, select the probes that are to be used for health monitoring in the list on the left, and then click <b>Add</b>. The selected probes appear in the list on the right.</p> <div>  <p><b>Note</b> The probe must have the same IP address type (IPv6 or IPv4) as the real server. For example, you cannot configure an IPv6 probe to an IPv4 real server.</p> </div> <p>The redirect real server probe list contains only configured probes of the type <i>Is Routed</i>, which means that the ACE routes the probe address according to the ACE internal routing table (see the <a href="#">“Configuring Health Monitoring for Real Servers”</a> section on page 6-41).</p> <div>  <p><b>Note</b> The Probes field list on the left does not display the VM probe type.</p> </div> <p>To remove probes that you do not want to use for health monitoring, select them in the list on the right, and then click <b>Remove</b>. The selected probes appear in the list on the left.</p> |

Table 6-1 Real Server Attributes (continued)

| Field           | Description                                                                                                                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rate Bandwidth  | The bandwidth rate is the number of bytes per second and applies to the network traffic exchanged between the ACE and the real server in both directions.<br><br>Specify the real server bandwidth limit in bytes per second. Valid entries are integers from 1 to 300000000. |
| Rate Connection | The connection rate is the number of connections per second received by the ACE and applies only to new connections destined to a real server.<br><br>Specify the limit for connections per second. Valid entries are integers from 1 to 350000.                              |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Real Servers table.
- Click the **Add another** icon to save your entries and to configure another real server.

**Step 5** To display statistics and status information for an existing real server, choose a real server from the Real Servers table, and then click **Details**. The **show rserver name detail** CLI command output appears. See the “[Displaying Real Server Statistics and Status Information](#)” section on page 6-8 for details.

#### Related Topics

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [Configuring Server Farms, page 6-18](#)
- [Configuring Sticky Groups, page 7-11](#)

## Displaying Real Server Statistics and Status Information

You can display statistics and status information for a particular real server.

#### Procedure

**Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Real Servers**.

The Real Servers table appears.

**Step 2** In the Real Servers table, choose a real server from the Real Servers table, and click **Details**.

The **show rserver name detail** CLI command output appears. For details on the displayed output fields, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*, Chapter 2, “Configuring Real Servers and Server Farms.”

**Step 3** Click **Update Details** to refresh the output for the **show rserver name detail** CLI command. The new information appears in a separate panel with a new timestamp; both the old and the new real server statistics and status information appear side-by-side to avoid overwriting the last updated information.

**Step 4** Click **Close** to return to the Real Servers table.

---

#### Related Topics

- [Configuring Real Servers, page 6-5](#)
- [Managing Real Servers, page 6-9](#)
- [Viewing All Real Servers, page 6-12](#)

## Managing Real Servers

The Real Servers table (**Config > Operations > Real Servers**) provides the following information by default for each server:

- Server name
- IP address
- Port
- Associated virtual server
- Associated virtual context
- Admin State (In Service, Out Of Service, or In Service Standby)
- Operational state (See [Table 6-3](#) for descriptions of real server operational states.)
- Number of current connections
- Current server weight
- Locality
- Stat Age, time as the page load since the SNMP values were polled
- Associated server farm

In the table, Disabled indicates that either the information is not available from the database or that it is not being collected via SNMP. To identify any SNMP-related issues, select the real server's virtual context in the object selector. If there are problems with SNMP, SNMP status will appear in the upper right above the content pane.

The following options are available from the Real Servers table:

- [Activating Real Servers, page 6-10](#)
- [Suspending Real Servers, page 6-10](#)
- [Modifying Real Servers, page 6-11](#)
- [Viewing All Real Servers, page 6-12](#)

## Activating Real Servers

Use this procedure to activate a real server.

### Procedure

- 
- Step 1** Choose **Config > Operations > Real Servers**. The Real Servers table appears.
- Step 2** Select the servers that you want to activate, and then click **Activate**. The Activate Server screen appears.
- Step 3** In the Task field, confirm that this is the server that you want to activate.
- Step 4** In the Reason field, enter a reason for this action. You might enter a trouble ticket, an order ticket, or a user message.



**Caution** Do not enter a password in this field.

---

- Step 5** Do the following:
- Click **Deploy Now** to deploy this configuration and to return to the Real Servers table. The server appears in the table with the status Inservice.
  - Click **Cancel** to exit this procedure without activating the server and to return to the Real Servers table.
- 

### Related Topics

- [Managing Real Servers, page 6-9](#)
- [Suspending Real Servers, page 6-10](#)
- [Viewing All Real Servers, page 6-12](#)

## Suspending Real Servers

Use this procedure to suspend a real server.

### Procedure

- 
- Step 1** Choose **Config > Operations > Real Servers**. The Real Servers table appears.
- Step 2** Select the server that you want to suspend, and then click **Suspend**. The Suspend Server screen appears.
- Step 3** In the Reason field, enter the reason for this action. You might enter a trouble ticket, an order ticket, or a user message. **Do not enter a password in this field.**
- Step 4** Select one of the following from the Type drop down menu:
- Graceful
  - Suspend
  - Suspend and Clear Connections to clear the existing connections to this server as part of the shutdown process

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration and to return to the Real Servers table. The server appears in the table with the status Out Of Service.
  - Click **Cancel** to exit this procedure without suspending the server and to return to the Real Servers table.
- 

#### Related Topics

- [Managing Real Servers, page 6-9](#)
- [Activating Real Servers, page 6-10](#)
- [Viewing All Real Servers, page 6-12](#)

## Modifying Real Servers

Use this procedure to modify weight and connection limits for real servers.

#### Procedure

---

- Step 1** Select the servers whose configuration you want to modify, and then click **Change Weight** below the table to the right of **Activate** and **Suspend**. The **Change Weight Real Servers** window appears.
- Step 2** Enter the following information for the selected server:
- Reason for change—Such as trouble ticket, order ticket or user message. **Do not enter a password in this field.**
  - Weight—Select a value from 1 to 100.
- Step 3** Do the following:
- Click **Deploy Now** to accept your entries and to return to the Real Servers table. The server appears in the table with the updated information.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Real Servers table.
- 

#### Related Topics

- [Managing Real Servers, page 6-9](#)
- [Activating Real Servers, page 6-10](#)
- [Viewing All Real Servers, page 6-12](#)

## Viewing All Real Servers

To view all real servers, choose **Config > Operations > Real Servers**. The Real Servers table displays the following information in [Table 6-2](#) by default:

**Table 6-2** *Real Server Table Fields*

| Item        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | Real server name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IP address  | Real server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Port        | Port used to by the real server for communications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Vservers    | Associated virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Context     | Associated virtual context.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Admin       | Administrative state of the real server: In Service, Out Of Service, or In Service Standby.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Oper        | Operational state of the real server (see <a href="#">Table 6-3</a> for descriptions of real server operational states).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Conn        | Number of current connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Wt          | Current server weight.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Locality    | <p>Locality requires that you configure the Dynamic Workload Scaling on the ACE (see the “<a href="#">Configuring Dynamic Workload Scaling</a>” section on page 6-14).</p> <p>Location of the real server, which must be a VM and not a physical server. Possible locality states are as follows:</p> <ul style="list-style-type: none"> <li>• N/A—he ACE cannot determine the real server location (local or remote). A possible cause for this issue is that Dynamic Workload Scaling is not configured correctly.</li> <li>• Local—The real server is located in the local network.</li> <li>• Remote—The real server is located in the remote network. The ACE bursts traffic to this server when the CPU or memory usage of the local real server reaches the specified maximum threshold value.</li> </ul> |
| Stat Age    | Time as of the page load when the SNMP values were polled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Farm | Associated server farm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

In the previous table, Disabled indicates that either the information is not available from the database or that it is not being collected via SNMP. To identify any SNMP-related issues, select the real server’s virtual context in the object selector. If there are problems with SNMP, SNMP status will appear in the upper right above the content pane.

**Table 6-3** *Real Server Operational States*

| State               | Description                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------|
| ARP Failed          | An ARP request to this server has failed.                                                                                       |
| Failed              | The server has failed and will not be retried for the amount of time specified by its retry timer.                              |
| Inactive            | The server is disabled as it has become inactive such as in the case when the real server is not associated to any server farm. |
| Inband probe failed | The server has failed the inband Health Probe agent.                                                                            |

**Table 6-3** *Real Server Operational States (continued)*

| State                     | Description                                                                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inservice                 | The server is in use as a destination for server load balancing client connections.                                                                        |
| Inservice standby         | The server is in standby state. No connections will be assigned to it unless the primary server fails.                                                     |
| Max. Load                 | The server is under maximum load and cannot receive any additional connections.                                                                            |
| ND Failed                 | For IPv6, Neighbor Discovery (ND) was unable to resolve the address of the real server.                                                                    |
| Operation wait            | The server is ready to become operational but is waiting for the associated redirect virtual server to be in service.                                      |
| Out of service            | The server is not in use by a server load balancer as a destination for client connections.                                                                |
| Probe failed              | The server load-balancing probe to this server has failed. No new connections will be assigned to this server until a probe to this server succeeds.       |
| Probe testing             | The server has received a test probe from the server load balancer.                                                                                        |
| Ready to test             | The server has failed and its retry timer has expired; test connections will begin flowing to it soon.                                                     |
| Return code failed        | The server has been disabled because it returned an HTTP code that matched a configured value.                                                             |
| Test wait                 | The server is ready to be tested. This state is applicable only when the server is used for HTTP redirect load balancing.                                  |
| Testing                   | The server has failed and has been given another test connection. The success of this connection is not known.                                             |
| Throttle: DFP             | <a href="#">DFP</a> has lowered the weight of the server to throttle level; no new connections will be assigned to the server until DFP raises its weight. |
| Throttle: max clients     | The server has reached its maximum number of allowed clients.                                                                                              |
| Throttle: max connections | The server has reached its maximum number of connections and is no longer being given connections.                                                         |
| Unknown                   | The state of the server is not known.                                                                                                                      |

**Related Topics**

- [Activating Real Servers, page 6-10](#)
- [Suspending Real Servers, page 6-10](#)
- [Modifying Real Servers, page 6-11](#)

# Configuring Dynamic Workload Scaling

This section describes how to configure the ACE Dynamic Workload Scaling (DWS) feature. DWS enables an ACE to burst traffic to a remote pool of VMs when the average CPU or memory usage of the local VMs has reached a specified maximum threshold value. When the usage drops to a specified minimum threshold value, the ACE stops bursting traffic to the remote VMs. For more information about the Dynamic Workload Scaling feature, see the [“Dynamic Workload Scaling Overview” section on page 6-4](#).

DWS requires configuring an ACE with the following:

- Nexus 7000 Series switches—XML interface IP address of the local Cisco Nexus 7000 series switches that the ACE polls to obtain VM location information (local or remote).



**Note** With Device Manager software Version A5(1.2), you can specify up to two Nexus 7000 switches that the ACE is to poll. With Device Manager software Version A5(1.1), you can specify only one Nexus 7000 switch.

- VM Controller—IP address of the VM Controller (also known as VMware vCenter Server) that the ACE sends a health probe to monitor local VM load.
- VM probe—Probe that the ACE sends to the VM Controller to monitor local VM load based on CPU usage, memory usage, or both (see the [“Configuring Health Monitoring” section on page 6-39](#)).
- Server Farms—Groups of networked real servers (physical servers and VMs) that provide content delivery. See the [“Configuring Server Farms” section on page 6-18](#).



**Note**

To enable the ACE to use the VMs associated with DWS for load balancing, you must configure them as real servers on the ACE (see the [“Configuring Real Servers” section on page 6-5](#)).

## Prerequisites

Dynamic Workload Scaling requires the following configuration elements:

- A Cisco Nexus 7000 Series switch configured for DCI/OTV in the local data center and in the remote data center. For details about configuring a Nexus 7000 for DCI/OTV, see the *Cisco Nexus 7000 NX-OS OTV Configuration Guide, Release 5.x*.
- VMware vCenter Server 4.0 or later.
- Multiple local and remote VMs configured as real servers and associated with server farms configured on the ACE.
- ACE backend interface MTU set to 1430 or less to accommodate DCI encapsulation and the Don't Fragment (DF) bit is automatically set on the DCI link. For details about setting the ACE MTU, see the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.

This section contains the following topics:

- [Configuring and Verifying a Cisco Nexus 7000 Connection, page 6-15](#)
- [Configuring and Verifying a VM Controller Connection, page 6-16](#)



## Configuring and Verifying a Cisco Nexus 7000 Connection

This procedure describes how to configure an ACE with the Cisco Nexus 7000 Series switch attributes required to allow the ACE to communicate with the Cisco Nexus 7000 Series switch using SSH. The ACE uses the Cisco Nexus 7000 Series switch to obtain VM location information (local or remote).

**Note**

With Device Manager software Version A5(1.2), you can specify up to two Cisco Nexus 7000 Series switches that the ACE is to poll. With Device Manager software Version A5(1.1), you can specify only one Cisco Nexus 7000 Series switch.

You can also use this procedure to edit the attributes of an existing Cisco Nexus 7000 Series switch profile or remove a switch profile.

**Guidelines and Restrictions**

Configure up to two Cisco Nexus 7000 Series switches per ACE in the Admin context.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > Load Balancing > Dynamic Workload Scaling > Nexus 7000 Setup**.

The Nexus 7000 Setup pane appears.

**Note**

If existing Cisco Nexus 7000 Series switch profiles already exist, the Name field lists their profile names in drop-down list on the right.

- Step 2** From the Nexus 7000 Setup pane, do one of the following:

- Define a new Cisco Nexus 7000 Series switch profile as follows:
  - a. From the Name field, click the text box radio button if it is not already selected and enter a Nexus 7000 name with a maximum of 64 characters. See the [Note](#) at the beginning of this chapter for ACE object naming specifications.
  - b. From the Primary IP field, enter the Cisco Nexus 7000 Series XML interface IP address in dotted-decimal format (such as 192.168.11.1).
  - c. From the User Name field, enter the username that the ACE uses for access and authentication on the Nexus 7000. Valid entries are unquoted text strings with a maximum of 64 characters with no spaces.

**Note**

The user must have either the vdc-admin or network-admin role to receive the Nexus 7000 output for the VM location information in XML format.

- d. From the Password field, enter the password that the ACE uses for authentication on the Nexus 7000. Valid entries are unquoted text strings with a maximum of 64 characters with no spaces.
  - e. From the Confirm field, reenter the password and go to [Step 3](#).
- Edit an existing Cisco Nexus 7000 Series switch profile as follows:

- a. From the Name field, click the radio button for the drop down list that contains the list of existing switch profile names.
- b. From the drop down list, choose the switch profile to edit. The current profile attributes display.
- c. Edit the profile fields as described in the procedure above for creating a new profile and go to [Step 3](#).

**Step 3** Click **Deploy Now** to deploy this configuration on the ACE and save your entry to the running-configuration and startup-configuration files. If you specified a new switch profile, it is added to the drop down list located in the Name field.

**Note**

Configuring the ACE for Dynamic Workload Scaling also requires configuring the ACE with the VM Controller information (see [“Configuring and Verifying a VM Controller Connection” section on page 6-16](#)) and configuring a VM health probe (see the [“Configuring Health Monitoring” section on page 6-39](#)).

**Step 4** (Optional) Use the function buttons available from this window as follows:

- Click **Details** to verify connectivity between the ACE and the selected Nexus 7000 switch profile.  
The ACE **show nexus-device device\_name detail** CLI command output displays in a pop-up window and includes the device name, IP address, and connection information. For more information about the command output, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.
- Click **Delete** to delete the currently selected Nexus 7000 switch profile.

**Caution**

If the ACE is currently configured for Dynamic Workload Scaling, deleting a Nexus 7000 switch profile disables the feature if only one switch profile is defined.

**Related Topics**

- [Configuring and Verifying a VM Controller Connection, page 6-16](#)
- [Configuring Health Monitoring, page 6-39](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)
- [Dynamic Workload Scaling Overview, page 6-4](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Server Farms, page 6-18](#)

## Configuring and Verifying a VM Controller Connection

This procedure describes how to configure an ACE with the VM Controller (VMware vCenter Server) attributes required to allow the ACE to communicate with the VM Controller to obtain local VM load information.

**Guidelines and Restrictions**

Configure only one VM Controller per ACE Admin context.

**Prerequisites**

The ACE is configured to communicate with the local Nexus 7000 that enables the ACE to discover the locality of the VM Controller VMs (see the [“Configuring and Verifying a Cisco Nexus 7000 Connection”](#) section on page 6-15).

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > Load Balancing > Dynamic Workload Scaling > VM Controller Setup**.

The VM Controller Setup pane appears.

- Step 2** From the VM Controller Setup pane, define the VM Controller using the information in [Table 6-4](#).

**Table 6-4** *VM Controller Setup*

| Field     | Description                                                                                                                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name      | VM Controller name (see the <a href="#">Note</a> at the beginning of this chapter for ACE object naming specifications).                                                                                                                            |
| URL       | IP address or URL for the VM Controller web services API agent. The URL must point to the VM Controller software development kit (SDK), for example, <a href="https://1.2.3.4/sdk">https://1.2.3.4/sdk</a> . Enter a maximum of 255 characters.     |
| User Name | Username that the ACE uses for access and authentication on the VM Controller. The user must have a read-only role at least or a role with a read privilege. Valid entries are unquoted text strings with a maximum of 64 characters and no spaces. |
| Password  | Password to be used for authentication on the VM Controller. Valid entries are unquoted text strings with a maximum of 64 characters and no spaces.<br>Reenter the password in the Confirm field.                                                   |

- Step 3** Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.



**Note** Configuring the ACE for Dynamic Workload Scaling also requires configuring the ACE with the Nexus 7000 information (see [“Configuring and Verifying a Cisco Nexus 7000 Connection”](#) section on page 6-15) and configuring a VM health probe (see the [“Configuring Health Monitoring”](#) section on page 6-39).

- Step 4** (Optional) Click **Details** to verify connectivity between the ACE and the remote VM Controller.  
The ACE **show vm-controller device\_name detail** CLI command output displays in a pop-up window and includes VM Controller status, IP address, and connection information.

- Step 5** (Optional) Click **Delete** to delete the currently configured VM Controller.



**Note** If the ACE is currently configured to use the Dynamic Workload Scaling, before you can delete the VM controller, you must delete the associated VM health probe (see the [“Configuring Health Monitoring”](#) section on page 6-39).

**Related Topics**

- [Configuring and Verifying a Cisco Nexus 7000 Connection, page 6-15](#)
- [Configuring Health Monitoring, page 6-39](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)
- [Dynamic Workload Scaling Overview, page 6-4](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Server Farms, page 6-18](#)

## Configuring Server Farms

Server farms are groups of networked real servers (physical servers and VMs) that contain the same content and that typically reside in the same physical location in a data center.

**Note**

With Dynamic Workload Scaling configured on the ACE, the real servers that are VMs can also reside in a remote datacenter (see the [“Configuring Dynamic Workload Scaling” section on page 6-14](#)).

Web sites often comprise groups of servers configured in a server farm. Load-balancing software distributes client requests for content or services among the real servers based on the configured policy and traffic classification, server availability and load, and other factors. If one server goes down, another server can take its place and continue to provide the same content to the clients who requested it.

**Note**

A server farm can support a mix of IPv6 and IPv4 real servers, and can be associated with both IPv6 and IPv4 probes.

Use this procedure to configure load balancing on server farms.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Server Farms**.  
The Server Farms window appears. For information about this window, see the [“Viewing All Server Farms” section on page 6-38](#)).
- Step 2** Click **Add** to add a new server farm, or select an existing server farm, and then click **Edit**.  
The Server Farms configuration screen appears.
- Step 3** Enter the server farm attributes (see [Table 6-5](#)).

**Table 6-5**      *Server Farm Attributes*

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | Either accept the automatically incremented value in this field, or enter a unique name for this server farm. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Type        | <p>Select the type of server farm:</p> <ul style="list-style-type: none"> <li>• Host—Indicates that this is a typical server farm that consists of real servers that provide content and services to clients</li> <li>• Redirect—Indicates that this server farm consists only of real servers that redirect client requests to alternate locations specified in the real server configuration. (See <a href="#">Configuring Real Servers, page 6-5</a>.)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                           |
| Description | Enter a brief description for this server farm. Valid entries are unquoted alphanumeric text strings with no spaces and a maximum of 240 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Fail Action | <p>Select the action the ACE appliance is to take with respect to connections if any real server in the server farm fails:</p> <ul style="list-style-type: none"> <li>• N/A—Indicates that the ACE appliance is to take no action if any server in the server farm fails.</li> <li>• Purge—Indicates that the ACE appliance is to remove connections to a real server if that real server in the server farm fails. The ACE appliance sends a reset command to both the client and the server that failed.</li> <li>• Reassign—The ACE is to reassign the existing server connections to the backup real server (if configured) if the real server fails after you enter this command. If a backup real server has not been configured for the failing server, this selection leaves the existing connections untouched in the failing real server.</li> </ul> |

Table 6-5 Server Farm Attributes (continued)

| Field                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failaction Reassign Across Vlans | <p>This field appears only when the Fail Action is set to Reassign.</p> <p>Check the check box to specify that the ACE reassigns the existing server connections to the backup real server on a different VLAN interface (commonly referred to as a bypass VLAN) if the real server fails. If a backup real server has not been configured for the failing server, this option has no effect and leaves the existing connections untouched in the failing real server.</p> <p>Note the following configuration requirements and restrictions when you enable this option:</p> <ul style="list-style-type: none"> <li>• Enable the Transparent option (see the next Field) to instruct the ACE not to use NAT to translate the ACE VIP address to the server IP address. The Failaction Reassign Across Vlans option is intended for use in stateful firewall load balancing (FWLB) on your ACE, where the destination IP address for the connection coming in to the ACE is for the end-point real server, and the ACE reassigns the connection so that it is transmitted through a different next hop.</li> <li>• Enable the MAC Sticky option on all server-side interfaces to ensure that packets that are going to and coming from the same server in a flow will traverse the same firewalls or stateful devices (see the <a href="#">“Configuring Virtual Context VLAN Interfaces”</a> section on page 10-10).</li> <li>• Configure the Predictor Hash Address option. See the <a href="#">“Configuring the Predictor Method for Server Farms”</a> section on page 6-29 for the supported predictor methods and configurable attributes for each predictor method.</li> <li>• You must configure identical policies on the primary interface and the backup-server interface. The backup interface must have the same feature configurations as the primary interface.</li> <li>• If you configure a policy on the backup-server interface that is different from the policies on the primary-server interface, that policy will be effective only for new connections. The reassigned connection will always have only the primary-server interface policies.</li> <li>• Interface-specific features (for example, NAT, application protocol inspection, outbound ACLs, or SYN cookie) are not supported.</li> <li>• You cannot reassign connections to the failed real server after it comes back up. This restriction also applies to same-VLAN backup servers.</li> <li>• Real servers must be directly connected to the ACE. This requirement also applies to same-VLAN backup server.</li> <li>• You must disable sequence number randomization on the firewall (see the <a href="#">“Configuring Connection Parameter Maps”</a> section on page 8-5).</li> <li>• Probe configurations should be similar on both ACEs and the interval values should be low. For example, if you configure a high interval value on ACE-1 and a low interval value on ACE-2, the reassigned connections may become stuck because of the probe configuration mismatch. ACE-2 with the low interval value will detect the primary server failure first and will reassign all its incoming connections to the backup-server interface VLAN. ACE-1 with the high interval value may not detect the failure before the primary server comes back up and will still point to the primary server.</li> </ul> <p>To minimize packet loss, we recommend the following probe parameter values on both ACEs: Interval: 2, Faildetect: 2, Passdetect interval: 2, and Passdetect count: 5.</p> |

Table 6-5 Server Farm Attributes (continued)

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic Workload Scaling | <p>This field appears only for host server farms.</p> <p>Allows the ACE to burst traffic to remote VMs when the average CPU or memory usage of the local VMs has reached its specified maximum threshold value. The ACE stops bursting traffic to the remote VMs when the average CPU or memory usage of the local VMs has dropped below its specified minimum threshold value. This option requires that you configure the ACE for Dynamic Workload Scaling using a Cisco Nexus 7000 Series switch, VM Controller, and VM probe (see the <a href="#">“Configuring Dynamic Workload Scaling”</a> section on page 6-14).</p> <p>Click one of the following radio button options:</p> <ul style="list-style-type: none"> <li>• N/A—Not applicable (default).</li> <li>• Local—Restricts the ACE to use of local VMs only for server load balancing.</li> <li>• Burst—Enables the ACE to burst traffic to remote VMs when needed.</li> </ul> <p>When you choose Burst, the VM Probe Name field appears along with a list of available VM probes. Choose an available VM probe or click <b>Add</b> to display the Health Monitoring pop-up window and create a new VM probe or edit an existing one (see the <a href="#">“Configuring Health Monitoring”</a> section on page 6-39).</p> |
| Fail-On-All              | <p>This field appears only for host server farms.</p> <p>By default, real servers that you configure in a server farm inherit the probes that you configure directly on that server farm. When you configure multiple probes on a server farm, the real servers in the server farm use an OR logic with respect to the probes, which means that if one of the probes configured on the server farm fails, all the real servers in that server farm fail and enter the PROBE-FAILED state. With AND logic, if one server farm probe fails, the real servers in the server farm remain in the operational state. If all the probes associated with the server farm fail, then all the real servers in that server farm fail and enter the PROBE-FAILED state.</p> <p>Click this check box to configure the real servers in a server farm to use AND logic with respect to multiple server farm probes.</p> <p>The Fail-On-All function is applicable to all probe types.</p>                                                                                                                                                                                                                                                                                                          |

Table 6-5 Server Farm Attributes (continued)




| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inband-Health Check                | <p>This field appears only for host server farms.</p> <p>By default, the ACE monitors the health of all real servers in a configuration through the use of ARPs and health probes. However, there is latency period between when the real server goes down and when the ACE becomes aware of the state. The inband health monitoring feature allows the ACE to monitor the health of the real servers in the server farm through the following connection failures:</p> <ul style="list-style-type: none"> <li>For TCP, resets (RSTs) from the server or SYN timeouts.</li> <li>For UDP, ICMP Host, Network, Port, Protocol, and Source Route unreachable messages.</li> </ul> <p>When you configure the failure-count threshold and the number of these failures exceeds the threshold within the reset-time interval, the ACE immediately marks the server as failed, takes it out of service, and removes it from load balancing. The server is not considered for load balancing until the optional resume-service interval expires.</p> <p>Choose one of the following:</p> <ul style="list-style-type: none"> <li>Count—Tracks the total number of TCP or UDP failures, and increments the counters as displayed by the <b>show serverfarm name inband</b> CLI command.</li> <li>Log—Logs a syslog error message when the number of events reaches the configured connection failure threshold.</li> <li>Remove—Logs a syslog error message when the number of events reaches the threshold and removes the server from service.</li> </ul> <p> <b>Note</b> You can configure this feature and health probes to monitor a server. When you do, both are required to keep a real server in service within a server farm. If either feature detects a server is out of service, the ACE does not select the server for load balancing.</p> |
| Connection Failure Threshold Count | <p>This field appears only when the Inband-Health Check is set to Log or Remove.</p> <p>Enter the maximum number of connection failures that a real server can exhibit in the reset-time interval before ACE marks the real server as failed. Valid entries are integers from 1 to 4294967295.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Reset Timeout (Milliseconds)       | <p>This field appears only when the Inband-Health Check is set to Log or Remove.</p> <p>Enter the number of milliseconds for the reset-time interval. Valid entries are integers from 100 to 300000. The default interval is 100.</p> <p>This interval starts when the ACE detects a connection failure. If the connection failure threshold is reached during this interval, the ACE generates a syslog message. When Inband-Health Check is set to Remove, the ACE also removes the real server from service.</p> <p>Changing the setting of this option affects the behavior of the real server, as follows:</p> <ul style="list-style-type: none"> <li>When the real server is in the OPERATIONAL state, even if several connection failures have occurred, the new reset-time interval takes effect the next time that a connection error occurs.</li> <li>When the real server in the INBAND-HM-FAILED state, the new reset-time interval takes effect the next time that a connection error occurs after the server transitions to the OPERATIONAL state.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



Table 6-5 Server Farm Attributes (continued)

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resume Service (Seconds)     | <p>This field appears only when the Inband-Health Check is set to Remove.</p> <p>Enter the number of seconds after a server has been marked as failed to reconsider it for sending live connections. Valid entries are integers from 30 to 3600. By default, this field is not configured. The setting of this option affects the behavior of the real server in the inband failed state, as follows:</p> <ul style="list-style-type: none"> <li>When this field is not configured, the real server remains in the failed state until you manually suspend and then reactivate it.</li> <li>When this field is not configured and then you configure this option with an integer between 30 and 3,600, the failed real server immediately transitions to the Operational state.</li> <li>When you configure this field and then increase the value, the real server remains in the failed state for the duration of the previously-configured value. The new value takes effect the next time the real server transitions to the failed state.</li> <li>When you configure this field and then decrease the value, the failed real server immediately transitions to the Operational state.</li> <li>When you configure this field with an integer between 30 and 3,600 and then reset it deleting the value from the field, the real server remains in the failed state for the duration of the previously-configured value. The unconfigured setting takes effect the next time the real server transitions to the failed state. Then the real server remains in the failed state until you manually suspend and then reactivate it.</li> <li>When you change this field within the reset-time interval and the real server is in the OPERATIONAL state with several connection failures, the new threshold interval takes effect the next time that a connection error occurs, even if it occurs within the current reset-time interval.</li> </ul> |
| Transparent                  | <p>This field appears only for real servers identified as host servers.</p> <p>Check the check box to specify that network address translation from the VIP address to the server IP is to occur. Clear the check box to indicates that network address translation from the VIP address to the server IP address is not to occur (default).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Partial-Threshold Percentage | <p>This field appears only for host server farms.</p> <p>Enter the minimum percentage of real servers in the primary server farm that must remain active for the server farm to stay up. If the percentage of active real servers falls below this threshold, the ACE takes the server farm out of service. Valid entries are integers from 0 to 99.</p> <p>After you configure a value in this field, enter a value in the Back Inservice field to bring the primary server farm back into service.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 6-5 Server Farm Attributes (continued)

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Back Inservice | <p>This field appears only for host server farms.</p> <p>Enter the percentage of real servers in the primary server farm that must be active again for the ACE to place the server farm back into service. Valid entries are integers from 0 to 99. The value in this field must be greater than or equal the value in the Partial Threshold Percentage field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Probes         | <p>In the Available list, choose the probes to use for health monitoring, and click <b>Add</b>. The selected probes appear in the Selected list.</p> <p>The redirect server farm probe list contains only configured probes of the type Is Routed, which means that the ACE routes the probe address according to the ACE internal routing table (see the <a href="#">“Configuring Health Monitoring for Real Servers”</a> section on page 6-41).</p> <div>  <p><b>Note</b> You can associate both IPv6 and IPv4 probes to a server farm.</p> </div> <div>  <p><b>Note</b> The list of Available probes does not display the VM probe type. To choose a VM probe for monitoring local VM usage, see the <a href="#">Dynamic Workload Scaling</a> field.</p> </div> <p>To remove probes that you do not want to use for health monitoring, select them in the Selected list, and then click <b>Remove</b>. The selected probes appear in the Available list.</p> |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. To add real servers to the farm and to configure server farm attributes, see the following topics:
  - [Adding Real Servers to a Server Farm, page 6-26](#)
  - [Configuring Health Monitoring, page 6-39](#)
  - [Configuring Server Farm HTTP Return Error-Code Checking, page 6-36](#)
- Click **Cancel** to exit the procedure without saving your entries and to return to the Server Farms table.
- Click **Next** to save your entries and to configure another server farm.

**Step 5** (Optional) To display statistics and status information for an existing server farm, choose a server farm from the Server Farms table, and click **Details**.

The **show serverfarm name detail** CLI command output appears. See the [“Displaying Server Farm Statistics and Status Information”](#) section on page 6-39 for details.

**Related Topics**

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Sticky Groups, page 7-11](#)
- [Configuring Health Monitoring, page 6-39](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 6-36](#)

- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Adding Real Servers to a Server Farm

After adding a server farm, (see [Configuring Server Farms, page 6-18](#)), you can associate real servers with it and configure predictors and retcode maps. The configuration screens for these attributes appear beneath the Server Farms table or after you have successfully added a new server farm.



### Note

If you do not see these tabs beneath the Server Farms table, click the **Switch between Configure and Browse Modes** button.

When creating or editing a server farm, if the real server to be added has the same name as an existing global real server but contains a different IP address (or no IP address), the Device Manager displays the following error message:

IP address of pre-existing real sever cannot be changed: "<rs-name>" (ip-addr).

If this error message appears, ensure that you specify an existing real server with the matching IP address.

Use this procedure to add real servers to a server farm.

### Assumptions

- A server farm has been added to the ACE Appliance Device Manager. (See [Configuring Server Farms, page 6-18](#).)
- At least one real server exists.

### Consideration

A server farm can support a mix of IPv6 and IPv4 real servers.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Server Farms**. The Server Farms table appears.
- Step 2** Select the server farm you want to associate with real servers, and then select the Real Servers tab. The Real Servers table appears.
- Step 3** Click **Add** to add a new entry to the Real Servers table, or select an existing server, and then click **Edit** to modify it. The Real Servers configuration screen appears.
- Step 4** Configure the real server using the information in [Table 6-6](#).


**Table 6-6** Real Server Configuration Attributes

| Field              | Description                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name               | Select the server that you want to associate with the server farm.                                                                                                           |
| Port               | Enter the port number to be used for server port address translation (PAT). Valid entries are integers from 1 to 65535.                                                      |
| Backup Server Name | Select the server that is to act as the backup server for the server farm. Leave this field blank to indicate that there is no designated backup server for the server farm. |
| Backup Server Port | If you select a backup server, enter the backup server port number. Valid entries are integers from 1 to 65535.                                                              |

Table 6-6 Real Server Configuration Attributes (continued)

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| State                 | <p>Select the state of this server:</p> <ul style="list-style-type: none"> <li>• In Service—Indicates that this server is in service.</li> <li>• In Service Standby—Indicates that this server is a backup server and is to remain inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.</li> <li>• Out Of Service—Indicates that this server is out of service.</li> </ul>                                                                                                                                                                                                                                                                                             |
| Buddy Real Group Name | Create a buddy real server group or select an existing one to enable persistence to the same real server or group of real servers across multiple server farms (for more information, see the <a href="#">“Buddy Sticky Groups” section on page 7-6</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Fail-On-All           | <p>This field appears only for real servers identified as host servers.</p> <p>By default, real servers with multiple probes configured for them have an OR logic associated with them. This means that if one of the real server probes fails, the real server fails and enters the PROBE-FAILED state.</p> <p>Click this check box to configure a real server to remain in the OPERATIONAL state unless all probes associated with it fail (AND logic).</p> <p>The Fail On All function is applicable to all probe types.</p>                                                                                                                                                                                                                             |
| Min. Connections      | Enter the minimum number of connections that the number of connections must fall below before the ACE appliance resumes sending connections to the server after it has exceeded the number in the Max. Connections field. The number in this field must be less than or equal to the number in the Max. Connections field. 1 to 4000000. The default value is 4000000.                                                                                                                                                                                                                                                                                                                                                                                      |
| Max. Connections      | Enter the maximum number of active connections that can be sent to the server. When the number of connections exceeds this number, the ACE appliance stops sending connections to the server until the number of connections falls below the number specified in the Min. Connections field. Valid entries are integers from 1 to 4000000. The default is 4000000.                                                                                                                                                                                                                                                                                                                                                                                          |
| Weight                | Enter the weight to assign to the server. Valid entries are integers from 1 to 100, and the default is 8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cookie String         | <p>This field appears only for real servers identified as hosts.</p> <p>Enter a cookie string value of the real server, which is to be used for HTTP cookie insertion when establishing a sticky connection. Valid entries are text strings with a maximum of 32 alphanumeric characters. You can include spaces and special characters in a cookie string value.</p> <p>Use cookie insertion when you want to use a session cookie for persistence if the server is not currently setting the appropriate cookie. With this feature enabled, the ACE inserts the cookie in the Set-Cookie header of the response from the server to the client. See <a href="#">Chapter 7, “Configuring Stickiness”</a> for details on HTTP cookie sticky connections.</p> |

Table 6-6 Real Server Configuration Attributes (continued)

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Probes          | <p>Select the probes in the Available list that you want to apply to this server, and then click <b>Add</b>. The selected probes appear in the Selected list. To remove probes you do not want to apply to this server, select the probes in the Selected list, and then click <b>Remove</b>.</p> <p> <b>Note</b> The Available list does not display the VM probe type.</p> |
| Rate Bandwidth  | <p>The bandwidth rate is the number of bytes per second and applies to the network traffic exchanged between the ACE and the real server in both directions.</p> <p>Specify the bandwidth limit in bytes per second. Valid entries are integers from 1 to 300000000.</p>                                                                                                                                                                                      |
| Rate Connection | <p>The connection rate is the number of connections per second received by the ACE and applies only to new connections destined to a real server.</p> <p>Specify the limit for connections per second. Valid entries are integers from 1 to 350000.</p>                                                                                                                                                                                                       |

**Step 5** When you finish configuring this server for this server farm, click:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit this procedure without saving your entries and to return to the Real Servers table.
- **Next** to save your entries and to add another real server for this server farm.

#### Related Topics

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Sticky Groups, page 7-11](#)
- [Configuring Health Monitoring, page 6-39](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 6-36](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Configuring the Predictor Method for Server Farms

After adding a server farm, ([Configuring Server Farms, page 6-18](#)), you can associate real servers with it and configure the predictor method and retcode maps. The configuration screens for these attributes appear beneath the Server Farms table or after you have successfully added a new server farm.

**Note**

If you do not see these tabs beneath the Server Farms table, click the **Switch between Configure and Browse Modes** button.

Use this procedure to configure the predictor method for a server farm. The predictor method specifies how the ACE appliance is to select a server in the server farm when it receives a client request for a service.

**Note**

You can configure only one predictor method per server farm.

### Assumptions

- A server farm has been added to the ACE Appliance Device Manager. (See [Configuring Server Farms, page 6-18](#).)
- At least one real server exists.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Server Farms**. The Server Farms table appears.
- Step 2** Select the server farm you want to configure the predictor method for, and then select the Predictor tab. The Predictor configuration screen appears.
- Step 3** In the Type field, select the method that the ACE appliance is to use to select a server in this server farm when it receives a client request. [Table 6-7](#) lists the available options and describes them.
- Step 4** Enter the required information for the selected predictor method. Round Robin is the default predictor method. See [Table 6-7](#).

Table 6-7 Predictor Method Attributes


| Predictor Method | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash Address     | <p>The ACE selects the server using a hash value based on the source or destination IP address.</p> <p>To configure the hash address predictor method:</p> <ol style="list-style-type: none"> <li>In the Mask Type field, indicate whether server selection is based on source IP address or the destination IP address: <ul style="list-style-type: none"> <li>N/A—This option is not defined.</li> <li>Destination—The server is selected based on the destination IP address.</li> <li>Source—The server is selected based on the source IP address.</li> </ul> </li> </ol> <p> <b>Note</b> If you configure the server farm with IPv6 and IPv4 Hash Address predictors at the same time, both predictors must have the same mask type.</p> <ol style="list-style-type: none"> <li>In the IP Netmask field, select the subnet mask to apply to the address. If none is specified, the default is 255.255.255.255.</li> <li>In the IPv6 Prefix-Length field, enter the IPv6 prefix length. If none is specified, the default is 128.</li> </ol> |



Table 6-7 Predictor Method Attributes (continued)

| Predictor Method      | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash Content          | <p>The ACE selects the server by using a hash value based on the specified content string of the HTTP packet body.</p> <ol style="list-style-type: none"> <li>1. In the Begin Pattern field, enter the beginning pattern of the content string and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</li> </ol> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> <ol style="list-style-type: none"> <li>2. In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</li> </ol> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> <ol style="list-style-type: none"> <li>3. In the Length field, enter the length in bytes of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes.</li> </ol> <p>The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.</p> <p>You cannot specify both the length and the end-pattern options for a Hash Content predictor.</p> <ol style="list-style-type: none"> <li>4. In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.</li> </ol> |
| Hash Cookie           | <p>The ACE selects the server by using a hash value based on the cookie name.</p> <p>In the Cookie Name field, enter a cookie name in the form of an unquoted text string with no spaces and a maximum of 64 characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Hash Secondary Cookie | <p>The ACE selects the server by using the hash value based on the specified cookie name in the URL query string, not the cookie header.</p> <p>In the Cookie Name field, enter a cookie name in the form of an unquoted text string with no spaces and a maximum of 64 characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Table 6-7 Predictor Method Attributes (continued)

| Predictor Method | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash Header      | <p>The ACE selects the server by using a hash value based on the header name.</p> <p>In the Header Name field, select the HTTP header to be used for server selection:</p> <ul style="list-style-type: none"> <li>To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button and enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</li> <li>To specify one of the standard HTTP headers, select the second radio button, then select one of the HTTP headers from the list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Hash Layer4      | <p>The ACE selects the server by using a Layer 4 generic protocol load-balancing method. Use this predictor to load balance packets from protocols that are not explicitly supported by the ACE.</p> <ol style="list-style-type: none"> <li>In the Begin Pattern field, enter the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions.<br/> <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions.<br/> <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> </li> <li>In the Length field, enter the length in bytes of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. <p>The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.</p> <p>You cannot specify both the length and end-pattern options for a Hash Layer 4 predictor.</p> </li> <li>In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.</li> </ol> |

Table 6-7 Predictor Method Attributes (continued)

| Predictor Method  | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash URL          | <p>The ACE selects the server using a hash value based on the URL. Use this method to load balance firewalls.</p> <p>Enter values in one or both of the pattern fields:</p> <ul style="list-style-type: none"> <li>In the URL Begin Pattern field, enter the beginning pattern of the URL and the pattern string to parse.</li> <li>In the URL End Pattern field, enter the ending pattern of the URL and the pattern string to parse.</li> </ul> <p>Valid entries for these fields are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters for each pattern you configure. The following special characters are also allowed: @ # \$</p> |
| Least Bandwidth   | <p>The ACE selects the server with the least amount of network traffic over a specified sampling period.</p> <ol style="list-style-type: none"> <li>In the Assess Time field, enter the number of seconds for which the ACE is to collect traffic information. Valid entries are integers from 1 to 10 seconds.</li> <li>In the Least Bandwidth Samples field, enter the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).</li> </ol>                                                              |
| Least Connections | <p>The ACE selects the server with the fewest number of connections.</p> <p>In the Slow Start Duration field, enter the slow-start value to be applied to this predictor method. Valid entries are integers from 1 to 65535, where 1 is the slowest ramp-up value.</p> <p>The slow-start mechanism is used to avoid sending a high rate of new connections to servers that you have just put into service.</p>                                                                                                                                                                                                                                                          |

Table 6-7 Predictor Method Attributes (continued)

| Predictor Method | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Least Loaded     | <p>The ACE selects the server with the lowest load based on information from SNMP probes.</p> <ol style="list-style-type: none"> <li>In the SNMP Probe Name field, select the name of the SNMP probe to use.</li> <li>In the Auto Adjust field, configure the autoadjust feature to instruct the ACE to apply the maximum load of 16000 to a real server whose load reaches zero or override the default behavior. By default, the ACE applies the average load of the server farm to a real server whose load is zero. The ACE periodically adjusts this load value based on feedback from the server SNMP probe and other configured options.</li> </ol> <p>Options are as follows:</p> <ul style="list-style-type: none"> <li>Average—Applies the average load of the server farm to a real server whose load is zero. This setting allows the server to participate in load balancing, while preventing it from being flooded by new connections. This is the default setting.</li> <li>Maxload—Instruct the ACE to apply the maximum load of 16000 to a real server whose load reaches zero.</li> <li>Off—Instruct the ACE to send all new connections to the server that has a load of zero until the next load update arrives from the SNMP probe for this server. If two servers have the same lowest load (either zero or nonzero), the ACE load balances the connections between the two servers in a round-robin manner.</li> </ul> <ol style="list-style-type: none"> <li>In the Weight Connection field, check the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.</li> </ol> <p>To instruct the ACE to select the server with the lowest load, use the predictor least-loaded command in server farm host or redirect configuration mode. With this predictor, the ACE uses SNMP probes to query the real servers for load parameter values (for example, CPU utilization or memory utilization). This predictor is considered adaptive because the ACE continuously provides feedback to the load-balancing algorithm based on the behavior of the real server.</p> <p>To use this predictor, you must associate an SNMP probe with it. The ACE queries user-specified OIDs periodically based on a configurable time interval. The ACE uses the retrieved SNMP load value to determine the server with the lowest load.</p> <p>The syntax of this predictor command is as follows:</p> <p><b>predictor least-loaded probe <i>name</i></b></p> <p>The name argument specifies the identifier of the existing SNMP probe that you want the ACE to use to query the server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.</p> <p>For example, to configure the ACE to select the real server with the lowest load based on feedback from an SNMP probe called PROBE_SNMP, enter:</p> <pre>host1/Admin(config)# <b>serverfarm SF1</b> host1/Admin(config-sfarm-host)# <b>predictor least-loaded probe PROBE_SNMP</b> host1/Admin(config-sfarm-host-predictor)#</pre> <p>To reset the predictor method to the default of Round Robin, enter:</p> <pre>host1/Admin(config-sfarm-host)# <b>no predictor</b></pre> |

Table 6-7 Predictor Method Attributes (continued)

| Predictor Method | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Response         | <p>The ACE selects the server with the lowest response time for a requested response-time measurement.</p> <ol style="list-style-type: none"> <li>In the Response Type field, select the type of measurement to use: <ul style="list-style-type: none"> <li>App-Req-To-Resp—The response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.</li> <li>Syn-To-Close—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server.</li> <li>Syn-To-Synack—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a SYN-ACK from the server.</li> </ul> </li> <li>In the Response Samples field, enter the number of samples over which you want to average the results of the response-time measurement. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).</li> <li>In the Weight Connection field, check the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.</li> </ol> |
| Round Robin      | The ACE selects the next server in the list of servers based on server weight. This is the default predictor method.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Step 5** Click:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit this procedure without saving your entries and to return to the t Connection field table.

**Related Topics**

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Sticky Groups, page 7-11](#)
- [Adding Real Servers to a Server Farm, page 6-26](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 6-36](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Configuring Server Farm HTTP Return Error-Code Checking

After adding a server farm, (see the “[Configuring Server Farms](#)” section on page 6-18), you can associate real servers with it and configure the predictor method and retcode maps. The configuration screens for these attributes appear beneath the Server Farms table or after you have successfully added a new server farm.

Use this procedure to configure HTTP return error-code checking (retcode map) for a server farm.



### Note

This feature is available only for server farms configured as hosts. It is not available for server farms configured with the type Redirect.

### Assumption

A host type server farm has been added to the ACE Appliance Device Manager. (See [Configuring Server Farms](#), page 6-18.)

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Server Farms**. The Server Farms table appears.
- Step 2** Select the server farm you want to configure return error-code checking for, and then select the Retcode Map tab. The Retcode Map table appears. If you do not see tabs beneath the Server Farms table, click the **Switch Between Configure And Browse Modes** button.
- Step 3** Click **Add** to add a new entry to the table. The Retcode Map configuration screen appears.



### Note

You cannot modify an entry in the Retcode Map table. Instead, delete the existing entry, and then add a new one.

- Step 4** In the Lowest Retcode field, enter the minimum value for an HTTP return error code. Valid entries are integers from 100 to 599. This number must be less than or equal to the number in the Highest Retcode field.
- Step 5** In the Highest Retcode field, enter the maximum number for an HTTP return error code. Valid entries are integers from 100 to 599. This number must be greater than or equal to the number in the Lowest Retcode field.

**Step 6** In the Type field, specify the action to be taken and related options using the information in [Table 6-8](#).

**Table 6-8** *Return-Code Type Configuration Options*

| Option | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Count  | The ACE tracks the total number of return codes received for each return code number that you specify.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Log    | <p>The ACE generates a syslog error message when the number of events reaches a specified threshold.</p> <ol style="list-style-type: none"> <li>1. In the Threshold field, enter the number of events that the ACE is to receive before generating a syslog error message. Valid entries are integers from 1 to 4294967295.</li> <li>2. In the Reset field, enter the time interval in seconds for which the ACE checks for the return code. Valid entries are integers from 1 to 2147483647 seconds.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Remove | <p>The ACE generates a syslog error message when the number of events reaches a specified threshold and then removes the server from service.</p> <ol style="list-style-type: none"> <li>1. In the Threshold field, enter the number of events that the ACE is to receive before generating a syslog error message and removing the server from service. Valid entries are integers from 1 to 4294967295.</li> <li>2. In the Reset field, enter the time interval in seconds for which the ACE checks for the return code. Valid entries are integers from 1 to 2147483647 seconds.</li> <li>3. In the Resume Service field, enter the number of seconds that the ACE waits before it resumes service for the real server automatically after taking the real server out of service. Valid entries are 30 to 3600 seconds. By default, this field is not configured. The setting of this field affects the behavior of the real server in the failed state, as follows: <ul style="list-style-type: none"> <li>– When this field is not configured, the real server remains in the failed state until you manually remove it from service and read it.</li> <li>– When this field is not configured and then you configure it with an integer between 30 and 3,600, the failed real server immediately transitions to the Operational state.</li> <li>– When you configure this field and then increase the value, the real server remains in the failed state for the duration of the previously-configured value. The new value takes effect the next time the real server transitions to the failed state.</li> <li>– When you configure this field and then decrease the value, the failed real server immediately transitions to the Operational state.</li> <li>– When you configure this field with an integer between 30 and 3,600 and then reset it by deleting the value from the field, the real server remains in the failed state for the duration of the previously-configured value. The unconfigured setting takes effect the next time the real server transitions to the failed state. Then the real server remains in the failed state until you manually remove it from service and read it.</li> </ul> </li> </ol> |

**Step 7** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Retcode Map table.
- Click **Next** to save your entries and to add another retcode map.

#### Related Topics

- [Using Virtual Contexts, page 4-2](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)

- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Sticky Groups, page 7-11](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Viewing All Server Farms

Use this procedure to view all server farms associated with a virtual context.

### Procedure

---

**Step 1** Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

**Step 2** Choose the virtual context with the server farms that you want to view and choose **Load Balancing > Server Farms**.

The Server Farms table appears with the following information:

- Server farm name
- Server farm type (either host or redirect)
- Description

Depending on the server farms selected, additional tables appear below the Server Farms table. These tables include:

- **Real Servers**—Displays the real servers associated with the selected server farm.
- **Predictor**—Displays the selected predictor method for the selected server farm.
- **Retcode Map**—Displays the HTTP return error-code checking that has been configured for the selected server farm.

**Step 3** (Optional) Do the following:

- Add or edit a server farm (see the [“Configuring Server Farms” section on page 6-18](#))
  - Choose a server farm and click **Buddy Group** to view a pop-up window that displays the output of the **show buddy group** command. The pop-up window displays the list of buddy groups configured in the virtual context (for more information, see the [“Buddy Sticky Groups” section on page 7-6](#)).
  - Click the **Real Servers** tab to display the real servers associated with the selected server farm. From this tab you can manage the server farm real servers (see the [“Adding Real Servers to a Server Farm” section on page 6-26](#)).
  - Click the **Predictor** tab to display the predictor method associated with the selected server farm. From this tab you can choose the predictor method (see the [“Configuring the Predictor Method for Server Farms” section on page 6-29](#)).
  - Click the **Retcode Map** tab to display the HTTP return error-code checking that has been configured for the selected server farm. From this tab you can manage the error-code checking (see the [“Configuring Server Farm HTTP Return Error-Code Checking” section on page 6-36](#)).
-



**Related Topics**

- [Configuring Server Farms, page 6-18](#)
- [Adding Real Servers to a Server Farm, page 6-26](#)
- [Configuring Health Monitoring, page 6-39](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 6-36](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Displaying Server Farm Statistics and Status Information

You can display statistics and status information for a particular server farm.

**Procedure**

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; Load Balancing &gt; Server Farms</b> .<br>The Server Farms table appears.                                                                                                                                                                                                                                    |
| <b>Step 2</b> | In the Server Farms table, choose a server farm from the Server Farms table, and click <b>Details</b> .<br>The <b>show serverfarm name detail</b> CLI command output appears. For details about the displayed output fields, see the <i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i> , Chapter 2, Configuring Real Servers and Server Farms. |
| <b>Step 3</b> | Click <b>Update Details</b> to refresh the output for the <b>show serverfarm name detail</b> CLI command.<br>The new information appears in a separate panel with a new timestamp; both the old and the new server farm statistics and status information appear side-by-side to avoid overwriting the last updated information.                                      |
| <b>Step 4</b> | Click <b>Close</b> to return to the Server Farms table.                                                                                                                                                                                                                                                                                                               |
- 

**Related Topics**

- [Viewing All Server Farms, page 6-38](#)
- [Configuring Server Farms, page 6-18](#)
- [Adding Real Servers to a Server Farm, page 6-26](#)
- [Configuring Health Monitoring, page 6-39](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 6-36](#)
- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Configuring Health Monitoring

You can instruct the ACE appliance to check the health of servers and server farms by configuring health probes (sometimes referred to as *keepalives*). After you create a probe, you assign it to a real server or a server farm. A probe can be one of many types, including TCP, ICMP, Telnet, HTTP, and so on. You can also configure scripted probes using the TCL scripting language (see [TCL Scripts, page 6-40](#)).

The ACE appliance sends out probes periodically to determine the status of a server, verifies the server response, and checks for other network problems that may prevent a client from reaching a server. Based on the server response, the ACE appliance can place the server in or out of service, and, based on the status of the servers in the server farm, can make reliable load-balancing decisions.

Health monitoring on the ACE appliance tracks the state of a server by sending out probes. Also referred to as out-of-band health monitoring, the ACE appliance verifies the server response or checks for any network problems that can prevent a client to reach a server. Based on the server response, the ACE appliance can place the server in or out of service, and can make reliable load balancing decisions.

**Note**

You can configure the inband health monitoring feature and health probes to monitor the health of the real servers in a server farm. For more information on inband health monitoring, see the [“Configuring Server Farms” section on page 6-18](#).

The ACE appliance identifies the health of a server in the following categories:

- Passed—The server returns a valid response.
- Failed—The server fails to provide a valid response to the ACE or the ACE is unable to reach a server for a specified number of retries.

By configuring the ACE appliance for health monitoring, the ACE appliance sends active probes periodically to determine the server state.

The ACE appliance supports 4000 unique probe configurations which includes ICMP, TCP, HTTP, and other predefined health probes. The ACE appliance also allows the opening of 1000 sockets simultaneously.

**Related Topics**

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [TCL Scripts, page 6-40](#)

## TCL Scripts

The ACE appliance supports several specific types of health probes (for example HTTP, TCP, or ICMP health probes) when you need to use a diverse set of applications and health probes to administer your network. The basic health probe types supported in the current ACE appliance software release may not support the specific probing behavior that your network requires. To support a more flexible health-probing functionality, the ACE appliance allows you to upload and execute TCL scripts on the ACE appliance.

The TCL interpreter code in the ACE appliance is based on Release 8.44 of the standard TCL distribution. You can create a script to configure health probes. Script probes operate similar to other health probes available in the ACE appliance software. As part of a script probe, the ACE appliance executes the script periodically, and the exit code that is returned by the executing script indicates the relative health and availability of specific real servers. For information on health probes, see [Configuring Health Monitoring for Real Servers, page 6-41](#).

For your convenience, the following sample scripts for the ACE appliance are available to support the TCL feature and are supported by Cisco TAC:

- ECHO\_PROBE\_SCRIPT
- FINGER\_PROBE\_SCRIPT
- FTP\_PROBE\_SCRIPT

- HTTP\_PROBE\_SCRIPT
- HTTPCONTENT\_PROBE
- HTTPHEADER\_PROBE
- HTTPPROXY\_PROBE
- IMAP\_PROBE
- LDAP\_PROBE
- MAIL\_PROBE
- POP3\_PROBE
- PROBENOTICE\_PROBE
- RTSP\_PROBE
- SSL\_PROBE\_SCRIPT

These scripts are located in the probe: directory and are accessible in both the Admin and user contexts. Note that the script files in the probe: directory are read-only, so you cannot copy or modify them. However, you can copy files from the probe: directory. For more information, see the *Administration Guide, Cisco ACE Application Control Engine*.

To load a script into memory on the ACE appliance and enable it for use, use the **script file** command. For detailed information on uploading and executing Toolkit Command Language (TCL) scripts on the ACE appliance, refer to the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

## Configuring Health Monitoring for Real Servers

To check the health and availability of a real server, the ACE appliance periodically sends a probe to the real server. Depending on the server response, the ACE appliance determines whether to include the server in its load-balancing decision.



### Note

You can configure the inband health monitoring feature and health probes to monitor the health of the real servers in a server farm. When you do, both are required to keep a real server in service within a server farm. If either feature detects a server is out of service, the ACE does not select the server for load balancing. For more information on inband health monitoring, see the [“Configuring Server Farms” section on page 6-18](#).

Use this procedure to establish monitoring of real servers to determine their viability in load-balancing decisions.


### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Click **Add** to add a new health monitoring probe, or select an existing entry, and then click **Edit** to modify it. The Health Monitoring screen appears.
- Step 3** In the Name field, enter a name that identifies the probe and that associates the probe with the real server. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
- Step 4** In the Type field, select the type of probe you want to use. The probe type determines what the probe sends to the real server. See [Table 6-9](#) for the types of probes and their descriptions.

Table 6-9 Probe Types

| Probe Type | Description                                                                                                                                                                                                                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DNS        | Sends a request to a DNS server giving it a configured domain. To determine if the server is up, the ACE appliance must receive the configured IP address for that domain.                                                                                                                          |
| ECHO-TCP   | Sends a string to the server and compares the response with the original string. If the response string matches the original, the server is marked as passed. If not, the ACE appliance retries as configured before the server is marked as failed.                                                |
| ECHO-UDP   | Sends a string to the server and compares the response with the original string. If the response string matches the original, the server is marked as passed. If not, the ACE appliance retries as configured before the server is marked as failed.                                                |
| FINGER     | Sends a probe to the server to verify that a defined username is a username on the server.                                                                                                                                                                                                          |
| FTP        | Initiates an FTP session. By default, this probe is for an anonymous login with the option of configuring a user ID and password. The ACE appliance performs an FTP GET or LS to determine the outcome of the problem. This probe supports only active connections.                                 |
| HTTP       | Sets up a TCP connection and issues an HTTP request. Any valid HTTP response causes the probe to mark the real server as passed.                                                                                                                                                                    |
| HTTPS      | Similar to an HTTP probe, but this probe uses SSL to generate encrypted data.<br><br><b>Note</b> This option is not available for the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).                    |
| ICMP       | Sends an ICMP request and listens for a response. If the server returns a response, the ACE appliance marks the real server as passed. If there is no response and times out, or an ICMP standard error occurs, such as DESTINATION_UNREACHABLE, the ACE appliance marks the real server as failed. |
| IMAP       | Initiates an IMAP session, using a configured user ID and password. Then, the probe attempts to retrieve e-mail from the server and validates the result of the probe based on the return codes received from the server.                                                                           |
| POP        | Initiates a POP session, using a configured user ID and password. Then, the probe attempts to retrieve e-mail from the server and validates the result of the probe based on the return codes received from the server.                                                                             |
| RADIUS     | Connects to a RADIUS server and logs into it to determine if the server is up.                                                                                                                                                                                                                      |
| RTSP       | Establishes a TCP connection and sends a request packet to the server. The ACE compares the response with the configured response code to determine whether the probe succeeded.                                                                                                                    |
| Scripted   | Executes probes from a configured script to perform health probing. This method allows you to author specific scripts with features not present in standard probes.                                                                                                                                 |

Table 6-9 Probe Types (continued)

| Probe Type | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIP-TCP    | Establishes a TCP connection and sends an OPTIONS request packet to the user agent on the server. The ACE compares the response with the configured response code or expected string, or both, to determine whether the probe has succeeded. If you do not configure an expected status code, any response from the server is marked as failed.                                                              |
| SIP-UDP    | Establishes a UDP connection and sends an OPTIONS request packet to the user agent on the server. The ACE compares the response with the configured response code or expected string, or both, to determine whether the probe has succeeded. If you do not configure an expected status code, any response from the server is marked as failed.                                                              |
| SMTP       | Initiates an SMTP session by logging into the server.                                                                                                                                                                                                                                                                                                                                                        |
| SNMP       | Establishes a UDP connection and sends a maximum of eight SNMP OID queries to probe the server. The ACE weighs and averages the load information that is retrieved and uses it as input to the least-loaded algorithm for load-balancing decisions. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed. |
| TCP        | Initiates a TCP handshake and expects a response. By default, a successful response causes the probe to mark the server as passed. The probe then sends a FIN to end the session. If the response is not valid, or if there is no response, the probe marks the real server as failed.                                                                                                                       |
| TELNET     | Establishes a connection to the real server and verifies that a greeting from the application was received.                                                                                                                                                                                                                                                                                                  |
| UDP        | Sends a UDP packet to a real server. The probe marks the server as failed only if an ICMP Port Unreachable messages is returned.                                                                                                                                                                                                                                                                             |
| VM         | Sends a probe to the VMware VM Controller to determine the average amount of both CPU and memory usage of its associated local VMs. The probe response determines whether the ACE load-balances traffic to the local VMs only or bursts traffic to the remote VMs due to high usage of the local VMs.                                                                                                        |
|            |  <b>Note</b> Use a VM probe when you configure the ACE for Dynamic Workload Scaling (see the <a href="#">“Configuring Dynamic Workload Scaling”</a> section on page 6-14).                                                                                                                                                |

**Step 5** Enter health monitoring general attributes (see [Table 6-10](#)).



**Note**

Click **More Settings** to access the additional general attributes for the selected probe type. By default, the Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-10** *Health Monitoring General Attributes*





| Field                          | Action                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                    | Enter a description for this probe. Valid entries are unquoted alphanumeric text strings with no spaces and a maximum of 240 characters.                                                                                                                                                                                                                                         |
| Probe Interval (Seconds)       | <p>Enter the number of seconds that the ACE is to wait before sending another probe to a server marked as passed. Valid entries are from 2 to 65535 for all probe types except the VM probe, which has a range from 300 to 65535.</p> <p>The default is 15 for all probe types except the VM probe, which has a default of 300 seconds.</p>                                      |
| Pass Detect Interval (Seconds) | <p>Enter the number of seconds that the ACE is to wait before sending another probe to a server marked as failed. Valid entries are integers from 2 to 65535 with a default of 60.</p> <p> <b>Note</b> This field is not applicable for the VM probe type.</p>                                  |
| Fail Detect                    | <p>Enter the consecutive number of times that an ACE must detect that probes have failed to contact a server before marking the server as failed. Valid entries are integers from 1 to 65535 with a default of 3.</p> <p> <b>Note</b> This field is not applicable for the VM probe type.</p> |

Table 6-10 Health Monitoring General Attributes (continued)

| Field                                                       | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings (Not applicable for the VM probe type)</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Pass Detect Count                                           | Enter the number of successful probe responses from the server before the server is marked as passed. Valid entries are integers from 1 to 65535 with a default of 3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Receive Timeout (Seconds)                                   | Enter the number of seconds the ACE is to wait for a response from a server that has been probed before marking the server as failed. Valid entries are integers from 1 to 65535 with a default of 10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Destination IPv4/IPv6 Address <sup>1</sup>                  | <p>By default, the probe uses the IP address from the real or virtual server configuration for the destination IP address. To override the destination address that the probe uses, enter the preferred destination IP address in this field.</p> <div>  <p><b>Note</b> The following probes support IPv6 destination addresses: DNS, HTTP, HTTPS, ICMP, TCP, and UDP.</p> </div> <div>  <p><b>Note</b> When you assign a probe to a real server, they must be configured with the same IP address type (IPv6 or IPv4).</p> </div>                   |
| Is Routed <sup>2</sup>                                      | Check the check box to indicate that the destination IP address is routed according to the ACE internal routing table. Clear the check box to indicate that the destination IP address is not routed according to the ACE internal routing table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Port                                                        | <p>By default, the precedence in which the probe inherits the port number is as follows:</p> <ul style="list-style-type: none"> <li>• The port number that you configure for the probe.</li> <li>• The configured port number from the real server in server farm.</li> <li>• The configured port number from the VIP in a Layer 3 and Layer 4 class map.</li> <li>• The default port number. Table 6-11 lists the default port number for each probe type.</li> </ul> <p>If you explicitly configure a default port, the ACE always sends the probe to the default port. The probe does not dynamically inherit the port number from the real server in a server farm or from the VIP specified in the class map.</p> |

1. The Dest IP Address field is not applicable to the Scripted probe type.

2. The Is Routed field is not applicable to the RTSP, Scripted, SIP-TCP, and SIP-UDP probe types.

Table 6-11 Default Port Numbers for Probe Types

| Probe Type | Default Port Number |
|------------|---------------------|
| DNS        | 53                  |
| Echo       | 7                   |
| Finger     | 79                  |
| FTP        | 21                  |
| HTTP       | 80                  |

**Table 6-11**      *Default Port Numbers for Probe Types (continued)*

| Probe Type             | Default Port Number |
|------------------------|---------------------|
| HTTPS                  | 443                 |
| ICMP                   | Not applicable      |
| IMAP                   | 143                 |
| POP3                   | 110                 |
| RADIUS                 | 1812                |
| RTSP                   | 554                 |
| Scripted               | 1                   |
| SIP (both TCP and UDP) | 5060                |
| SMTP                   | 25                  |
| SNMP                   | 161                 |
| Telnet                 | 23                  |
| TCP                    | 80                  |
| UDP                    | 53                  |
| VM                     | 443                 |

**Step 6** Enter the attributes for the specific probe type selected:

- For DNS probes, see [Table 6-12](#).
- For Echo-TCP probes, see [Table 6-13](#).
- For Echo-UDP probes, see [Table 6-14](#).
- For Finger probes, see [Table 6-15](#).
- For FTP probes, see [Table 6-16](#).
- For HTTP probes, see [Table 6-17](#).
- For HTTPS probes, see [Table 6-18](#).
- There are no specific attributes for ICMP probes.
- For IMAP probes, see [Table 6-19](#).
- For POP probes, see [Table 6-20](#).
- For RADIUS probes, see [Table 6-21](#).
- For RTSP probes, see [Table 6-22](#).
- For Scripted probes, see [Table 6-23](#).
- For SIP-TCP probes, see [Table 6-24](#).
- For SIP-UDP probes, see [Table 6-25](#).
- For SMTP probes, see [Table 6-26](#).
- For SNMP probes, see [Table 6-27](#).
- For TCP probes, see [Table 6-28](#).
- For Telnet probes, see [Table 6-29](#).
- For UDP probes, see [Table 6-30](#).



- For VM probes, see [Table 6-31](#).

**Step 7** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Health Monitoring table.
- Click **Next** to save your entries and to configure another probe.

**Step 8** (Optional) To display statistics and status information for a particular probe, choose the probe from the Health Monitoring table, and click **Details**.

The **show probe name detail** CLI command output appears. See the “[Displaying Health Monitoring Statistics and Status Information](#)” section on [page 6-69](#) for details.

---

#### Related Topics

- [Configuring DNS Probe Expect Addresses, page 6-66](#)
- [Configuring Headers for HTTP and HTTPS Probes, page 6-66](#)
- [Configuring Health Monitoring Expect Status, page 6-67](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Server Farms, page 6-18](#)
- [Configuring Sticky Groups, page 7-11](#)

## Probe Attribute Tables

Refer to the following topics to configure health monitoring probe-specific attributes:

- [DNS Probe Attributes, page 6-48](#)
- [Echo-TCP Probe Attributes, page 6-48](#)
- [Echo-UDP Probe Attributes, page 6-49](#)
- [Finger Probe Attributes, page 6-49](#)
- [FTP Probe Attributes, page 6-50](#)
- [HTTP Probe Attributes, page 6-50](#)
- [HTTPS Probe Attributes, page 6-52](#)
- [IMAP Probe Attributes, page 6-54](#)
- [POP Probe Attributes, page 6-55](#)
- [RADIUS Probe Attributes, page 6-56](#)
- [RTSP Probe Attributes, page 6-56](#)
- [Scripted Probe Attributes, page 6-57](#)
- [SIP-TCP Probe Attributes, page 6-59](#)
- [SIP-UDP Probe Attributes, page 6-59](#)
- [SMTP Probe Attributes, page 6-60](#)
- [SNMP Probe Attributes, page 6-60](#)
- [TCP Probe Attributes, page 6-61](#)

- [Telnet Probe Attributes, page 6-62](#)
- [UDP Probe Attributes, page 6-63](#)
- [VM Probe Attributes, page 6-65](#)

Refer to the following topics for additional configuration options for health monitoring probes:

- [Configuring DNS Probe Expect Addresses, page 6-66](#)
- [Configuring Headers for HTTP and HTTPS Probes, page 6-66](#)
- [Configuring Health Monitoring Expect Status, page 6-67](#)
- [Configuring an OID for SNMP Probes, page 6-68](#)

## DNS Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the DNS probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-12** *DNS Probe Attributes*

| Field                | Action                                                                                                                                                                                                            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name          | Enter the domain name that the probe is to send to the DNS server. Valid entries are unquoted text strings with a maximum of 255 characters.                                                                      |
| <b>More Settings</b> |                                                                                                                                                                                                                   |
| Port                 | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description. |

To configure expect addresses for DNS probes, see [Configuring DNS Probe Expect Addresses, page 6-66](#).

## Echo-TCP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the Echo-TCP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-13** *Echo-TCP Probe Attributes*

| Field     | Action                                                                                                                                                |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Send Data | Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters. |

**Table 6-13** *Echo-TCP Probe Attributes (continued)*

| Field                      | Action                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings</b>       |                                                                                                                                                                                                                     |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST. |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                           |

## Echo-UDP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the Echo-UDP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-14** *Echo-UDP Probe Attributes*

| Field                | Action                                                                                                                                                                                                            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Send Data            | Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.                                                             |
| <b>More Settings</b> |                                                                                                                                                                                                                   |
| Port                 | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description. |

## Finger Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the Finger probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-15** *Finger Probe Attributes*

| Field                | Action                                                                                                                                                                                                            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Send Data            | Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.                                                             |
| <b>More Settings</b> |                                                                                                                                                                                                                   |
| Port                 | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description. |

**Table 6-15** *Finger Probe Attributes (continued)*

| Field                      | Action                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST. |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                           |

## FTP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the FTP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-16** *FTP Probe Attributes*

| Field                      | Action                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings</b>       |                                                                                                                                                                                                                     |
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.   |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST. |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                           |

To configure probe expect statuses for FTP probes, see [Configuring Health Monitoring Expect Status](#), page 6-67.

## HTTP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the HTTP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

Table 6-17 HTTP Probe Attributes

| Field                      | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Request Method Type        | Select the type of HTTP request method that is to be used for this probe: <ul style="list-style-type: none"> <li>N/A—This option is not defined.</li> <li>Get—The HTTP request method is a GET with a URL of “/”. This request method directs the server to get the page, and the ACE calculates a hash value for the content of the page. If the page content information changes, the hash value no longer matches the original hash value and the ACE assumes the service is down. This is the default request method.</li> <li>Head—The server is to only get the header for the page. Using this method can prevent the ACE from assuming that the service is down due to changed content and therefore changed hash values.</li> </ul> |
| Request HTTP URL           | This field appears if you select Head or Get in the Request Method Type field.<br><br>Enter the URL path on the remote server. Valid entries are strings of up to 255 characters specifying the URL path. The default path is “/”.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>More Settings</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Append Port Host Tag       | Check the check box to append port information in the HTTP Host header when you configure a non-default destination port for an HTTP probe. Clear the check box to not append the port information in the HTTP Host header.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| User Name                  | Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Password                   | Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.<br><br>Reenter the password in the Confirm field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Expect Regular Expression  | Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Expect Regex Offset        | Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regular Expression field. Valid entries are integers from 1 to 4000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 6-17 HTTP Probe Attributes (continued)

| Field       | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash        | Check the Hash check box to indicate that the ACE is to use an MD5 hash for an HTTP GET probe. Clear the Hash check box to indicate that the ACE should not use an MD5 hash for an HTTP GET probe.                                                                                                                                                                                                                                                                                                                                                      |
| Hash String | <p>This field appears if the Hash check box is selected.</p> <p>Enter the 32-bit hash value that the ACE is to compare with the hash that is generated from the HTTP page sent by the server. If you do not provide this value, the ACE generates a value the first time it queries the server, stores this value, and matches this value with other responses from the server. A successful comparison causes the probe to maintain an Alive state.</p> <p>Enter the MD5 hash value as a quoted or unquoted hexadecimal string with 16 characters.</p> |

To configure probe headers and expect statuses for HTTP probes, see the following topics:

- [Configuring Headers for HTTP and HTTPS Probes, page 6-66](#)
- [Configuring Health Monitoring Expect Status, page 6-67](#)

## HTTPS Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the HTTPS probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

Table 6-18 HTTPS Probe Attributes

| Field               | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Request Method Type | <p>Select the type of HTTP request method that is to be used for this probe:</p> <ul style="list-style-type: none"> <li>• N/A—This option is not defined.</li> <li>• Get—The HTTP request method is a GET with a URL of “/”. This request method directs the server to get the page, and the ACE calculates a hash value for the content of the page. If the page content information changes, the hash value no longer matches the original hash value and the ACE assumes the service is down. This is the default request method.</li> <li>• Head—The server is to only get the header for the page. Using this method can prevent the ACE from assuming that the service is down due to changed content and therefore changed hash values.</li> </ul> |

Table 6-18 HTTPS Probe Attributes (continued)

| Field                      | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Request HTTP URL           | <p>This field appears if you select Head or Get in the Request Method Type field.</p> <p>Enter the URL path on the remote server. Valid entries are strings of up to 255 characters specifying the URL path. The default path is “/”.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Cipher                     | <p>Select the cipher suite to be used with this HTTPS probe:</p> <ul style="list-style-type: none"> <li>• RSA_ANY—The HTTPS probe accepts all RSA-configured cipher suites and that no specific suite is configured. This is the default action.</li> <li>• RSA_EXPORT1024_WITH_DES_CBC_SHA</li> <li>• RSA_EXPORT1024_WITH_RC4_56_MD5</li> <li>• RSA_EXPORT1024_WITH_RC4_56_SHA</li> <li>• RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>• RSA_EXPORT_WITH_RC4_40_MD5</li> <li>• RSA_WITH_3DES_EDE_CBC_SHA</li> <li>• RSA_WITH_AES_128_CBC_SHA</li> <li>• RSA_WITH_AES_256_CBC_SHA</li> <li>• RSA_WITH_DES_CBC_SHA</li> <li>• RSA_WITH_RC4_128_MD5</li> <li>• RSA_WITH_RC4_128_SHA</li> </ul> |
| SSL Version                | <p>Select the version of SSL or TLS to be used in ClientHello messages sent to the server:</p> <ul style="list-style-type: none"> <li>• All—The probe is to use all SSL versions.</li> <li>• SSLv3—The probe is to use SSL version 3.</li> <li>• TLSv1—The probe is to use TLS version 1.</li> </ul> <p>By default, the probe sends ClientHello messages with an SSL version 3 header and a TLS version 1 message.</p>                                                                                                                                                                                                                                                                 |
| <b>More Settings</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Append Port Host Tag       | Check the check box to append port information in the HTTP Host header when you configure a non-default destination port for an HTTPS probe. Clear the check box to not append the port information in the HTTP Host header.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| User Name                  | Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 6-18 *HTTPS Probe Attributes (continued)*

| Field                         | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password                      | Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.<br>Reenter the password in the Confirm field.                                                                                                                                                                                                                                                                                                                                                      |
| Expect Regular Expression     | Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Expect Regex Offset           | Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regular Expression field. Value entries are integers from 1 to 4000.                                                                                                                                                                                                                                                                                                                                 |
| Hash                          | Check the Hash check box to indicate that the ACE is to use an MD5 hash for an HTTP GET probe. Clear this check box to indicate that the ACE is not to use an MD5 hash for an HTTP GET probe.                                                                                                                                                                                                                                                                                                                                                    |
| Hash String                   | This field appears if the Hash check box is selected.<br><br>Enter the 32-bit hash value that the ACE is to compare with the hash that is generated from the HTTP page sent by the server. If you do not provide this value, the ACE generates a value the first time it queries the server, stores this value, and matches this value with other responses from the server. A successful comparison causes the probe to maintain an Alive state.<br><br>Enter the MD5 hash value as a quoted or unquoted hexadecimal string with 16 characters. |
| Ignore Certificate Expiration | Check the Ignore Certificate Expiration check box to configure the probe to ignore the certificate expiration date so the probe does not affect ACE functionality when the certificate has expired. Uncheck the check box to configure the ACE not to ignore the certificate expiration date.                                                                                                                                                                                                                                                    |

To configure probe headers and expect statuses for HTTPS probes, see the following topics:

- [Configuring Headers for HTTP and HTTPS Probes, page 6-66](#)
- [Configuring Health Monitoring Expect Status, page 6-67](#)

## IMAP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the IMAP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.



**Table 6-19** *IMAP Probe Attributes*

| Field                      | Action                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Name                  | Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.                                                                |
| Password                   | Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.<br>Reenter the password in the Confirm field.                         |
| Mailbox Name               | Enter the user mailbox name from which to retrieve e-mail for this IMAP probe. Valid entries are unquoted text strings with a maximum of 64 characters.                                                             |
| Request Command            | Enter the request method command for this probe. Valid entries are text strings with a maximum of 32 characters and no spaces.                                                                                      |
| <b>More Settings</b>       |                                                                                                                                                                                                                     |
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.   |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST. |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                           |

**POP Probe Attributes****Note**

Click **More Settings** to access the additional attributes for the POP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-20** *POP Probe Attributes*

| Field                | Action                                                                                                                                                                                      |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Name            | Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.                                        |
| Password             | Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.<br>Reenter the password in the Confirm field. |
| Request Command      | Enter the request method command for this probe. Valid entries are text strings with a maximum of 32 characters and no spaces.                                                              |
| <b>More Settings</b> |                                                                                                                                                                                             |

**Table 6-20** *POP Probe Attributes (continued)*

| Field                      | Action                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.   |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST. |
| Open Timeout               | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                           |

## RADIUS Probe Attributes

**Note**

Click **More Settings** to access the additional attributes for the RADIUS probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-21** *RADIUS Probe Attributes*

| Field                | Action                                                                                                                                                                                                            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Secret          | Enter the shared secret to be used to allow probe access to the RADIUS server. Valid entries are case-sensitive strings with no spaces and a maximum of 64 characters.                                            |
| User Name            | Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.                                                              |
| Password             | Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.<br>Reenter the password in the Confirm field.                       |
| <b>More Settings</b> |                                                                                                                                                                                                                   |
| Port                 | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description. |
| NAS IP Address       | Enter the IP address of the Network Access Server (NAS) in dotted-decimal format, such as 192.168.11.1.                                                                                                           |

## RTSP Probe Attributes

**Note**

Click **More Settings** to access the additional attributes for the RTSP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

Table 6-22 RTSP Probe Attributes

| Field                           | Action                                                                                                                                                                                                                             |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                            | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                  |
| RTSP Require Header Value       | Enter the Require header for this probe.                                                                                                                                                                                           |
| RTSP Proxy Require Header Value | Enter the Proxy-Require header for this probe.                                                                                                                                                                                     |
| RTSP Request Method Type        | Select the request method type: <ul style="list-style-type: none"> <li>N/A—No request method is selected.</li> <li>Describe—This probe is to use the DESCRIBE request method.</li> </ul>                                           |
| Request HTTP URL                | This field appears if you select Describe in the RTSP Request Method Type field.<br><br>Enter the URL path for the URL request of the RTSP media stream on the server. Valid entries are strings with a maximum of 255 characters. |
| <b>More Settings</b>            |                                                                                                                                                                                                                                    |
| TCP Connection Termination      | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST.                |
| Open Timeout (Seconds)          | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                                          |

To configure probe expect statuses for RTSP probes, see [Configuring Health Monitoring Expect Status](#), page 6-67.


### Scripted Probe Attributes



#### Note

Click **More Settings** to access the additional attributes for the Scripted probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

Table 6-23 Scripted Probe Attributes

| Field                                           | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                                            | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Script Name                                     | <p>Enter the local name that you want to assign to this file on the ACE. This file can reside in the disk0: directory or the probe: directory (if the probe: directory exists).</p> <p> <b>Note</b> The script file must first be established on the ACE device and the name must be entered exactly as is appears on the device. Please refer to your ACE documentation for more details.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.</p>                                     |
| Script Arguments                                | Valid arguments are unquoted text strings with no spaces; separate multiple arguments with a space. The field limit is 255 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>More Settings</b>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Script Needs To Be Copied From Remote Location? | Check this check box to indicate that the file needs to be copied from a remote server. Clear this check box to indicate that the script resides locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Protocol                                        | <p>This field appears if the script is to be copied from a remote server.</p> <p>Select the protocol to be used for copying the script:</p> <ul style="list-style-type: none"> <li>• FTP—The script is to be copied using FTP.</li> <li>• TFTP—The script is to be copied using TFTP.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| User Name                                       | <p>This field appears if FTP is selected in the Protocol field.</p> <p>Enter the name of the user account on the remote server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Password                                        | <p>This field appears if FTP is selected in the Protocol field.</p> <p>Enter the password for the user account on the remote server.</p> <p>Reenter the password in the Confirm field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Source File Name                                | <p>This field appears if the script is to be copied from a remote server.</p> <p>Enter the host IP address, path, and filename of the file on the remote server in the format <i>host-ip/path/filename</i> where:</p> <ul style="list-style-type: none"> <li>• <i>host-ip</i> represents the IP address of the remote server.</li> <li>• <i>path</i> represents the directory path of the file on the remote server.</li> <li>• <i>filename</i> represents the filename of the file on the remote server.</li> </ul> <p>For example, your entry might resemble<br/> <b>192.168.11.2/usr/bin/my-script.ext.</b></p> |

## SIP-TCP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the SIP-TCP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-24** *SIP-TCP Probe Attributes*

| Field                      | Action                                                                                                                                                                                                                                                                                               |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings</b>       |                                                                                                                                                                                                                                                                                                      |
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                                                                                    |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST.                                                                                  |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                                                                                                            |
| Expect Regular Expression  | Enter the expected response data from the probe destination. Valid entries are text strings with a maximum of 255 characters. This field accepts both single and double quotes. Double quotes are considered delimiters so they don't appear on the device. Single quotes will appear on the device. |
| Expect Regex Offset        | Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regular Expression field. Value entries are integers from 1 to 4000.                                                                                     |

To configure probe expect statuses for SIP-TCP probes, see [Configuring Health Monitoring Expect Status](#), page 6-67.

## SIP-UDP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the SIP-UDP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-25** *SIP-UDP Probe Attributes*

| Field                | Action                                                                                                                                                                                                            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings</b> |                                                                                                                                                                                                                   |
| Port                 | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description. |

Table 6-25 SIP-UDP Probe Attributes (continued)

| Field                     | Action                                                                                                                                                                                                                                                                                               |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Rport              | Check the check box to indicate that the server will be forced to send a reply from the same port on which the request was received. Clear the check box to indicate that the server can send the reply from a different port than the port from which the request was received.                     |
| Expect Regular Expression | Enter the expected response data from the probe destination. Valid entries are text strings with a maximum of 255 characters. This field accepts both single and double quotes. Double quotes are considered delimiters so they don't appear on the device. Single quotes will appear on the device. |
| Expect Regex Offset       | Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regular Expression field. Value entries are integers from 1 to 4000.                                                                                     |

To configure probe expect statuses for SIP-UDP probes, see [Configuring Health Monitoring Expect Status](#), page 6-67.

## SMTP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the SMTP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

Table 6-26 SMTP Probe Attributes

| Field                      | Action                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings</b>       |                                                                                                                                                                                                                     |
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.   |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST. |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                           |

To configure probe expect statuses for SMTP probes, see [Configuring Health Monitoring Expect Status](#), page 6-67.

## SNMP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the SNMP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-27** *SNMP Probe Attributes*

| Field                | Action                                                                                                                                                                                                                            |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP Community       | Enter the SNMP community string. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.                                                                                                          |
| <b>More Settings</b> |                                                                                                                                                                                                                                   |
| Port                 | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                 |
| SNMP Version         | Select the SNMP version for this probe: <ul style="list-style-type: none"> <li>N/A—No version is selected.</li> <li>SNMPv1—This probe is to use SNMP version 1.</li> <li>SNMPv2c—This probe is to use SNMP version 2c.</li> </ul> |

To configure the SNMP OID for SNMP probes, see [Configuring an OID for SNMP Probes](#), page 6-68.

## TCP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the TCP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

**Table 6-28** *TCP Probe Attributes*

| Field                      | Action                                                                                                                                                                                                                                                                                                                          |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                                                                                                               |
| Send Data                  | Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.                                                                                                                                                                           |
| Send Hex Data              | Enter the data in hex format to be sent as part of probe request. The Hex data entered must be of even numbers and must be a single string consisting of alphanumeric within the range of 0-9,a-f or A-F, and a maximum of 254 characters. The conversion from Hex ASCII to Binary will happen when the probe data is sent out. |
| Data Format                | Users can enter only one data format either in “send-hex-data” or in “send-data” format. Click the radio button “send-hex-data” or “send-data” to choose the format. <b>Expect Regex / Expect Hex Regex</b> and <b>Expect Regex Offset / Expect Hex Regex Offset</b> shall be displayed based on the radio button selection.    |
| <b>More Settings</b>       |                                                                                                                                                                                                                                                                                                                                 |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST.                                                                                                             |

Table 6-28 TCP Probe Attributes (continued)

| Field                     | Action                                                                                                                                                                                                                                |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Open Timeout (Seconds)    | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                                             |
| Expect Regular Expression | Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.                                                                                        |
| Expect Regex Offset       | Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regular Expression field. Value entries are integers from 1 to 4000.                      |
| Expect Hex Regex          | Enter the expected response data from the probe destination. The Hex data entered must be of even numbers and must be a single string consisting of alphanumeric within the range of 0-9,a-f or A-F, and a maximum of 255 characters. |
| Expect Hex Regex Offset   | Enter the expected response data in Hex format. The Hex data entered must be of even numbered size and of maximum size of 254.                                                                                                        |

**CLI "expect ?"** will show both hex-regex and regex for user to configure, irrespective of type(ASCII or HEX) of send-data configured. TCP probe is created using CLI with Send-data and Expect hex-regex data with offset as given below:

```
switch/Admin(config)# probe tcp test1
switch/Admin(config-probe-tcp)# send-data "abcde"
switch/Admin(config-probe-tcp)# expect ?
hex-regex Configure Hex data expected as response
regex Configure probe expected response

switch/Admin(config-probe-tcp)# send-hex-data "abcd"
switch/Admin(config-probe-tcp)# expect ?
hex-regex Configure Hex data expected as response
regex Configure probe expected response
switch/Admin(config-probe-tcp)# expect
```

**Note**

If send-hex-data is configured then expect hex-regex should be configured. Similarly, if send-data is configured, expect regex should be configured.

## Telnet Probe Attributes

**Note**

Click **More Settings** to access the additional attributes for the Telnet probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.



Table 6-29 *Telnet Probe Attributes*

| Field                      | Action                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings</b>       |                                                                                                                                                                                                                     |
| Port                       | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.   |
| TCP Connection Termination | Check box that when checked, configures the ACE to terminate TCP connections gracefully by sending a FIN to the server. Uncheck the check box to configure the ACE to terminate a TCP connection by sending an RST. |
| Open Timeout (Seconds)     | Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 1.                                                           |

## UDP Probe Attributes



### Note

Click **More Settings** to access the additional attributes for the UDP probe type. By default, ACE appliance Device Manager hides the probe attributes with default values and the probe attributes which are not commonly used.

Table 6-30 *UDP Probe Attributes*

| Field                     | Action                                                                                                                                                                                                                                                                                                                          |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                      | Enter the port number that the probe is to use. By default, the probe uses port inheritance to determine the port number. For more information, see the general attribute <a href="#">Port</a> field description.                                                                                                               |
| Send Data                 | Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.                                                                                                                                                                           |
| Send Hex Data             | Enter the data in hex format to be sent as part of probe request. The Hex data entered must be of even numbers and must be a single string consisting of alphanumeric within the range of 0-9,a-f or A-F, and a maximum of 254 characters. The conversion from Hex ASCII to Binary will happen when the probe data is sent out. |
| Data Format               | Users can enter only one data format either in “send-hex-data” or in “send-data” format. Click the radio button “send-hex-data” or “send-data” to choose the format. <b>Expect Regex / Expect Hex Regex</b> and <b>Expect Regex Offset / Expect Hex Regex Offset</b> shall be displayed based on the radio button selection.    |
| <b>More Settings</b>      |                                                                                                                                                                                                                                                                                                                                 |
| Expect Regular Expression | Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.                                                                                                                                                                                  |
| Expect Regex Offset       | Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regular Expression field. Value entries are integers from 1 to 4000.                                                                                                                |

**Table 6-30** *UDP Probe Attributes (continued)*

| Field                   | Action                                                                                                                                                                                                                                |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Expect Hex Regex        | Enter the expected response data from the probe destination. The Hex data entered must be of even numbers and must be a single string consisting of alphanumeric within the range of 0-9,a-f or A-F, and a maximum of 255 characters. |
| Expect Hex Regex Offset | Enter the expected response data in Hex format. The Hex data entered must be of even numbered size and of maximum size of 254.                                                                                                        |

CLI "expect ?" will show both hex-regex and regex for user to configure, irrespective of type(ASCII or HEX) of send-data configured. UDP probe is created using CLI with Send-data and Expect hex-regex data with offset as given below:

```
switch/Admin(config)# probe udp test1
switch/Admin(config-probe-udp)# send-data "abcde"
switch/Admin(config-probe-udp)# expect ?
hex-regex Configure Hex data expected as response
regex Configure probe expected response

switch/Admin(config-probe-udp)# send-hex-data "abcd"
switch/Admin(config-probe-udp)# expect ?
hex-regex Configure Hex data expected as response
regex Configure probe expected response
switch/Admin(config-probe-udp)# expect
```

**Note**

If send-hex-data is configured then expect hex-regex should be configured. Similarly, if send-data is configured, expect regex should be configured.

## VM Probe Attributes



### Note

Use a VM probe when you configure the ACE for Dynamic Workload Scaling (see the [“Configuring Dynamic Workload Scaling”](#) section on page 6-14).

Configure the VM probe attributes to control when the ACE bursts traffic to remote VMs based on an average of local VM CPU usage, memory usage, or both. The ACE obtains the usage information by sending the VM probe to the specified VM Controller associated with the local VMs. It calculates the average aggregate load information for all local VMs as a percentage of CPU usage or memory usage and uses either or both percentages to determine when to burst traffic to the remote data center. If the server farm consists of both physical servers and VMs, the ACE considers load information only from the VMs.

By default, the VM probe checks the percentage of usage for either the CPU or memory against the maximum threshold value. Whichever percentage reaches its maximum threshold value first causes the ACE to burst traffic to the remote data center. The default maximum burst threshold value of 99 percent instructs the ACE to always load balance traffic to the local VMs unless the load value is equal to 100 percent or the VMs are not in the OPERATIONAL state. If you configure the maximum burst threshold value to 1 percent, the ACE always bursts traffic to the remote data center.

When the usage percentage is less than the minimum threshold value, the ACE stops bursting traffic to the remote data center and continues to load balance traffic to the local VMs. Any active connections to the remote data center are allowed to complete.

[Table 6-31](#) lists the VM probe attributes, which allow you to control when the ACE bursts traffic to remote VMs.

**Table 6-31** VM Probe Attributes

| Field                      | Action                                                                                                                                                                                                                                                                                          |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Probe Interval (seconds)   | Frequency in seconds with which the ACE sends probes to the VM controller. Enter an integer from 300 to 65535. The default is 300 (5 minutes).                                                                                                                                                  |
| Max CPU Burst Threshold    | Threshold for the maximum percentage of the CPU usage based on the average load information for all local VMs. When the CPU usage percentage reaches or exceeds this threshold, the ACE starts bursting traffic to the remote VMs. Enter a value from 1 to 99. The default is 99.               |
| Min CPU Burst Threshold    | Threshold for the minimum percentage of the CPU usage based on the average load information for all local VMs. When the CPU usage percentage drops below this threshold, the ACE stops bursting traffic to the remote VMs. Enter a value from 1 to 99 percent. The default is 99.               |
| Max Memory Burst Threshold | Threshold for the maximum percentage of the memory usage based on the average load information for all local VMs. When the memory usage percentage reaches or exceeds this threshold, the ACE starts bursting traffic to the remote VMs. Enter a value from 1 to 99 percent. The default is 99. |
| Min Memory Burst Threshold | Threshold for the minimum percentage of the memory usage based on the average load information for all local VMs. When the memory usage percentage drops below this threshold, the ACE stops bursting traffic to the remote VMs. Enter a value from 1 to 99 percent. The default is 99.         |
| VM Controller Name         | Identifier of the VM controller that you configured in the <a href="#">“Configuring and Verifying a VM Controller Connection”</a> section on page 6-16. Click the radio button for the VM controller.                                                                                           |

### Related Topics

- [Configuring Dynamic Workload Scaling, page 6-14](#)

## Configuring DNS Probe Expect Addresses


When a DNS probe sends a domain name resolve request to the server, it verifies the returned IP address by matching the received IP address with the configured addresses.

Use this procedure to specify the IP address that the ACE appliance expects to receive in response to a DNS request.

### Assumption

A DNS probe has been configured. See [Configuring Health Monitoring for Real Servers, page 6-41](#) for more information.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the DNS probe that you want to configure with an expected IP address. The Expect Addresses subtable appears.
- Step 3** Click **Add** to add an entry to the Expect Addresses table. The Expect Address configuration screen appears.
- 

**Note** You cannot modify an entry in the Expect Addresses table. Instead, delete the existing entry, and then add a new one.
- 
- Step 4** In the IPv4/IPv6 Address field, enter the IP address that the ACE appliance is to expect as a server response to a DNS request. You can enter multiple addresses in this field. However, you cannot mix IPv4 and IPv6 addresses.
- Step 5** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entry and to return to the Expect Addresses table.
  - Click **Next** to save your entry and to add another IP Address to the Expect Addresses table.
- 

### Related Topics

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [DNS Probe Attributes, page 6-48](#)

## Configuring Headers for HTTP and HTTPS Probes

Use this procedure to specify header fields for HTTP and HTTPS probes.

### Assumption

An HTTP or HTTPS probe has been configured. See [Configuring Health Monitoring for Real Servers, page 6-41](#) for more information.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the HTTP or HTTPS probe that you want to configure with header. The Probe Headers subtable appears.
- Step 3** Click **Add** to add an entry, or select an existing entry, and then click **Edit** to modify it. The Probe Headers configuration screen appears.
- Step 4** In the Header Name field, select the HTTP header the probe is to use.
- Step 5** In the Header Value field, enter the string to assign to the header field. Valid entries are text strings with a maximum of 255 characters. If the string includes spaces, enclose the string with quotes.
- Step 6** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entry and to return to the Probe Headers table.
  - Click **Next** to save your entry and to add another header entry to the Probe Headers table.
- 

### Related Topics

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [HTTP Probe Attributes, page 6-50](#)
- [HTTPS Probe Attributes, page 6-52](#)

## Configuring Health Monitoring Expect Status

When the ACE appliance receives a response from the server, it expects a status code to mark a server as passed. By default, there are no status codes configured on the ACE appliance. If you do not configure a status code, any response code from the server is marked as failed.

Expect status codes can be configured for FTP, HTTP, HTTPS, RTSP, SIP-TCP, SIP-UDP, and SMTP probes.

Use this procedure to configure a single or range of code responses that the ACE appliance expects from the probe destination.

### Assumption

An FTP, HTTP, HTTPS, RTSP, SIP-TCP, SIP-UDP, or SNMP probe has been configured. See [Configuring Health Monitoring for Real Servers, page 6-41](#) for more information.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the FTP, HTTP, HTTPS, or SMTP probe that you want to configure for expect status codes. The Expect Status subtable appears.

- Step 3** Click **Add** to add an entry, or select an existing entry, and then click **Edit** to modify it. The Expect Status configuration screen appears.
- Step 4** To configure a single expect status code:
- In the Min. Expect Status Code field, enter the expect status code for this probe. Valid entries are integers from 0 to 999.
  - In the Max. Expect Status code, enter the same expect status code that you entered in the Min. Expect Status Code field.
- Step 5** To configure a range of expect status codes:
- In the Min. Expect Status Code, enter the lower limit of the range of status codes. Valid entries are integers from 0 to 999.
  - In the Max. Expect Status Code, enter the upper limit of a range of status codes. Valid entries are integers from 0 to 999. The value in this field must be greater than or equal to the value in the Min. Expect Status Code field.
- Step 6** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Expect Status table.
  - Click **Next** to save your entries and to add another expect status code to the Expect Status table.
- 

#### Related Topics

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [FTP Probe Attributes, page 6-50](#)
- [HTTP Probe Attributes, page 6-50](#)
- [SNMP Probe Attributes, page 6-60](#)

## Configuring an OID for SNMP Probes

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

The ACE allows a maximum of eight OID queries to probe the server.

#### Assumption

An SNMP probe has been configured. See [Configuring Health Monitoring for Real Servers, page 6-41](#) for more information.

#### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the SNMP probe that you want to specify an OID for. The SNMP OID for Server Load Query table appears.

- Step 3** Click **Add** to add an entry, or select an existing entry, and then click **Edit** to modify it. The SNMP OID configuration pane appears.
- Step 4** In the SNMP OID field, enter the OID that the probe is to use to query the server for a value. Valid entries are unquoted strings with a maximum of 255 alphanumeric characters in dotted-decimal notation, such as .1.3.6.1.4.2021.10.1.3.1. The OID string is based on the server type.
- Step 5** In the Maximum Absolute Server Load Value field, enter the OID value in the form of an integer and to indicate that the retrieved OID value is an absolute value instead of a percent. Valid entries are integers from 1 to 4294967295.
- When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. By default, the ACE assumes that the retrieved OID value is a percentile value. Use this option to specify that the retrieved OID value is an absolute value.
- Step 6** In the Server Load Threshold Value field, specify the threshold at which the server is to be taken out of service:
- When the OID value is based on a percent, valid entries are integers from 1 to 100.
  - When the OID is based on an absolute value, valid entries are from 1 to the value specified in the Maximum Absolute Server Load Value field.
- Step 7** In the Server Load Weighting field, enter the weight to assign to this OID for the SNMP probe. Valid entries are integers from 0 to 16000.
- Step 8** Do the following:
- Click **Deploy Now** to deploy this configuration.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the SNMP OID table.
  - Click **Next** to deploy your entries and to add another item to the SNMP OID table.

#### Related Topics

- [Configuring Health Monitoring for Real Servers, page 6-41](#)
- [SNMP Probe Attributes, page 6-60](#)

## Displaying Health Monitoring Statistics and Status Information

You can display statistics and status information for a particular probe.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Health Monitoring**.  
The Health Monitoring table appears.
- Step 2** In the Health Monitoring table, choose a probe from the Health Monitoring table, and click **Details**.  
The **show probe name detail** CLI command output appears. For details on the displayed output fields, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*, Chapter 4, Configuring Health Monitoring.



**Note** For a DNS probe, the detailed probe results always identify a default DNS domain of www.Cisco.com.

- Step 3** Click **Update Details** to refresh the output for the **show probe name detail** CLI command.
- Step 4** Click **Close** to return to the Health Monitoring table.
- 

#### Related Topic

- [Configuring Health Monitoring for Real Servers, page 6-41](#)

## Configuring Secure KAL-AP

A keepalive-appliance protocol (KAL-AP) on the ACE allows communication between the ACE and the Global Site Selector (GSS), which send KAL-AP requests, to report the server states and loads for global-server load-balancing (GSLB) decisions. The ACE uses KAL-AP through a UDP connection to calculate weights and provide information for server availability to the KAL-AP device. The ACE acts as a server and listens for KAL-AP requests. When KAL-AP is initialized on the ACE, the ACE listens on the standard 5002 port for any KAL-AP requests. You cannot configure any other port.

The ACE supports secure KAL-AP for MD5 encryption of data between it and the GSS. For encryption, you must configure a shared secret as a key for authentication between the GSS and the ACE context.

When configuring a KAL-AP, you can use the wildcard KAL-AP GSS IP address (0.0.0.0) to establish a secure communications channel between the ACE and multiple GSS devices that use the same MD5 encryption secret.

Use this procedure to configure secure KAL-AP associated with a virtual context.

#### Assumptions

- You have created a virtual context that specifies the Keepalive Appliance Protocol over UDP.
- You have enabled KAL-AP on the ACE by configuring a management class map and policy map, and apply it to the appropriate interface.

#### Guidelines and Restrictions

Use the following guidelines and restrictions when using the 0.0.0.0 wildcard KAL-AP GSS IP address:

- Use the wildcard IP address when both the following conditions exist:
  - All GSS devices in the cluster use a secure channel for KAL-AP message exchange with ACE. Do not use the wildcard IP address if any GSS in the cluster uses an unsecure channel.
  - All or a set of GSS devices in the cluster use the same MD5 secret.



**Note** You can only use the wildcard VIP address for one set of GSS devices that use the same MD5 secret. You must configure all other GSS devices individually for KAL-AP.

---

- When removing a KAL-AP IP address, using the wildcard IP address removes only those GSS IP addresses that use the secret associated with the wildcard value. KAL-AP IP addresses that were defined using a specific GSS IP addresses remain and must be removed individually.

#### Procedure

---

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Secure KAL-AP**.



The Secure KAL-AP table appears.

- Step 2** Click **Add** to configure secure KAL-AP for MD5 encryption of data.

The Secure KAL-AP configuration screen appears.

- Step 3** In the IP Address field, enable secure KAL-AP by configuring the IP address for the GSS.

Using dotted-decimal notation (for example, 192.168.11.1), enter the IP address of a specific GSS device or enter the wildcard value (0.0.0.0) if all GSS devices in the cluster use the same MD5 encryption secret (see the [“Guidelines and Restrictions”](#) section on page 6-70).

In the Hash Key field, enter the MD5 encryption method shared secret between the KAL-AP device and the ACE. Enter the shared secret as a case-sensitive string with no spaces and a maximum of 31 alphanumeric characters. The ACE supports the following special characters in a shared secret:

, . / = + - ^ @ ! % ~ # \$ \* ( )

- Step 4** Do one of the following:

- Click **Deploy Now** to save your entries. The ACE appliance validates the secure KAL-AP configuration and deploys it.
- Click **Cancel** to exit this procedure without accepting your entries and to return to the Secure KAL-AP table.
- Click **Next** to accept your entries.

---

#### Related Topics

- [Creating Virtual Contexts](#), page 4-2
- [Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps](#), page 12-14





## CHAPTER 7

# Configuring Stickiness

---

This chapter provides an information about sticky behavior and procedures for configuring stickiness with an ACE appliance.



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

This chapter contains the following sections:

- [Stickiness Overview, page 7-1](#)
- [Configuring Sticky Groups, page 7-11](#)
- [Configuring Sticky Statics, page 7-21](#)

## Stickiness Overview

When customers visit an e-commerce site, they usually start out by browsing the site, the Internet equivalent of window shopping. Depending on the application, the site may require that the client become “stuck” to one server once the connection is established, or the application may not require this until the client starts to build a shopping cart.

In either case, once the client adds items to the shopping cart, it is important that all of the client requests get directed to the same server so that all the items are contained in one shopping cart on one server. An instance of a customer's shopping cart is typically local to a particular Web server and is not duplicated across multiple servers.

E-commerce applications are not the only types of applications that require stickiness. Any Web application that maintains client information may require stickiness, such as banking applications or online trading. Other uses include FTP and HTTP file transfers.

Stickiness allows the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session. A session, as used here, is defined as a series of transactions between a client and a server over some finite period of time (from several

minutes to several hours). This feature is particularly useful for e-commerce applications where a client needs to maintain multiple connections with the same server while shopping online, especially while building a shopping cart using HTTP requests and during the checkout process using HTTPS.

Depending on the configured SLB policy, the ACE appliance “sticks” a client to an appropriate server after the ACE appliance has determined which load-balancing method to use. If the ACE appliance determines that a client is already stuck to a particular server, then the ACE appliance sends that client request to that server, regardless of the load-balancing criteria specified by the matched policy. If the ACE appliance determines that the client is not stuck to a particular server, it applies the normal load-balancing rules to the content request.

You can configure stickiness to stick a client to a real server that is associated with a server farm or you can use the *buddy* sticky group feature to enable persistence to a real server or real server group across multiple server farms (see the “[Buddy Sticky Groups](#)” section on page 7-6).

For overview information on stickiness, see the following topics:

- [Sticky Types](#)
- [Sticky Groups](#)
- [Sticky Table](#)
- [Buddy Sticky Groups](#)

#### Related Topics

- [Configuring Virtual Server Layer 7 Load Balancing, page 5-30](#)
- [Configuring Sticky Groups, page 7-11](#)

## Sticky Types

The ACE appliance supports stickiness based on:

- HTTP cookies
- HTTP headers
- IP addresses
- HTTP content
- IP Netmask
- IPv6 Prefix
- Layer 4 payloads
- RADIUS attributes
- RTSP headers
- SIP headers
- SSL session ID

#### Related Topics

- [HTTP Content Stickiness, page 7-3](#)
- [HTTP Cookie Stickiness, page 7-3](#)
- [HTTP Header Stickiness, page 7-4](#)
- [IP Netmask and IPv6 Prefix Stickiness, page 7-4](#)

- [Layer 4 Payload Stickiness, page 7-4](#)
- [RADIUS Stickiness, page 7-5](#)
- [RTSP Header Stickiness, page 7-5](#)
- [SIP Header Stickiness, page 7-5](#)
- [SSL Stickiness, page 7-5](#)

## HTTP Content Stickiness

HTTP content stickiness allows you to stick a client to a server based on the content of an HTTP packet. You can specify a beginning pattern and ending pattern, the number of bytes to parse, and an offset that specifies how many bytes to ignore from the beginning of the data.

### Related Topics

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## HTTP Cookie Stickiness

Client *cookies* uniquely identify clients to the ACE and the servers providing content. A cookie is a small data structure within the HTTP header that is used by a server to deliver data to a Web client and request that the client store the information. In certain applications, the client returns the information to the server to maintain the connection state or persistence between the client and the server.

When the ACE examines a request for content and determines through policy matching that the content is sticky, it examines any cookie or URL present in the content request. The ACE uses the information in the cookie or URL to direct the content request to the appropriate server.

The ACE supports the following types of cookie stickiness:

- **Dynamic cookie learning**

You can configure the ACE to look for a specific cookie name and automatically learn its value either from the client request HTTP header or from the server Set-Cookie message in the server response. Dynamic cookie learning is useful when dealing with applications that store more than just the session ID or user ID within the same cookie. Only very specific bytes of the cookie value are relevant to stickiness.

By default, the ACE learns the entire cookie value. You can optionally specify an offset and length to instruct the ACE to learn only a portion of the cookie value.

Alternatively, you can specify a secondary cookie value that appears in the URL string in the HTTP request. This option instructs the ACE to search for (and eventually learn or stick to) the cookie information as part of the URL. URL learning is useful with applications that insert cookie information as part of the HTTP URL. In some cases, you can use this feature to work around clients that reject cookies.
- **Cookie insert**

The ACE inserts the cookie on behalf of the server upon the return request, so that the ACE can perform cookie stickiness even when the servers are not configured to set cookies. The cookie contains information that the ACE uses to ensure persistence to a specific real server.

**Related Topics**

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## HTTP Header Stickiness

You can use HTTP-header information to provide stickiness. With HTTP header stickiness, you can specify a header offset to provide stickiness based on a unique portion of the HTTP header.

**Related Topics**

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## IP Netmask and IPv6 Prefix Stickiness

You can use the source IP address, the destination IP address, or both to uniquely identify individual clients and their requests for stickiness purposes based on their IP netmask or IPv6 prefix. However, if an enterprise or a service provider uses a megaproxy to establish client connections to the Internet, the source IP address no longer is a reliable indicator of the true source of the request. In this case, you can use cookies or one of the other sticky methods to ensure session persistence.

**Related Topics**

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## Layer 4 Payload Stickiness

Layer 4 payload stickiness allows you to stick a client to a server based on the data in Layer 4 frames. You can specify a beginning pattern and ending pattern, the number of bytes to parse, and an offset that specifies how many bytes to ignore from the beginning of the data.

**Related Topics**

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## RADIUS Stickiness

RADIUS stickiness can be based on the following RADIUS attributes:

- Calling station ID
- Username

### Related Topics

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## RTSP Header Stickiness

RTSP stickiness is based on information in the RTSP session header. With RTSP header stickiness, you can specify a header offset to provide stickiness based on a unique portion of the RTSP header.

### Related Topics

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## SIP Header Stickiness

SIP header stickiness is based on the SIP Call-ID header field. SIP header stickiness requires the entire SIP header, so you cannot specify an offset.

### Related Topics

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## SSL Stickiness

SSL stickiness allows you to stick a client to a server based on the SSL session ID. You can associate an SSL sticky group with an HTTPS server load balancing policy map.

### Related Topics

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Groups, page 7-6](#)
- [Sticky Table, page 7-11](#)

## Sticky Groups

Sticky groups allow the ACE to keep a client stuck to a real server or group of real servers within a server farm. The ACE uses the concept of sticky groups to configure stickiness. A sticky group allows you to specify the sticky attributes. After you configure a sticky group and its attributes, you associate the sticky group with a Layer 7 policy-map action in a Layer 7 SLB policy map. You can create a maximum of 4096 sticky groups in each context. Each sticky group that you configure on the ACE appliance contains a series of parameters that determine the following:

- Sticky method
- Timeout
- Replication
- Cookie offset and other cookie-related attributes
- HTTP header offset and other header-related attributes
- Buddy group name

### Related Topics

- [Stickiness Overview, page 7-1](#)
- [Sticky Types, page 7-2](#)
- [Sticky Table, page 7-11](#)
- [Configuring Sticky Groups, page 7-11](#)

## Buddy Sticky Groups

Buddy sticky groups allow the ACE to keep a client stuck to a real server or group of real servers even when the client requests are processed by different server farms.

To use the buddy sticky group feature, you perform the following steps:

1. Create real server buddy groups when specifying the real servers in a server farm (see the [“Configuring Server Farms” section on page 6-18](#)).
2. Create sticky server farm buddy groups when specifying the server farms in a sticky group (see the [“Configuring Sticky Groups” section on page 7-11](#)). You make each sticky server farm to be buddied together a group *member*.

This section describes the following buddy sticky group applications:

- One-to-one association—Sticks the client to the same physical server instances in two different server farms.
- Asymmetric association—Sticks a client to a real server that is configured across different serverfarms even when the client comes back with a non-HTTP request or different HTTP header.
- Many-to-one association—Sticks multiple, first-tier real servers to one real server in a second tier that contains fewer servers.

This section includes the following topics:

- [Guidelines and Restrictions, page 7-7](#)
- [One-to-One Association Example, page 7-7](#)
- [Asymmetric Association Example, page 7-8](#)



- [Many-to-One Association Example, page 7-9](#)

## Guidelines and Restrictions

Observe the following guidelines and restrictions when using the buddy sticky group feature:

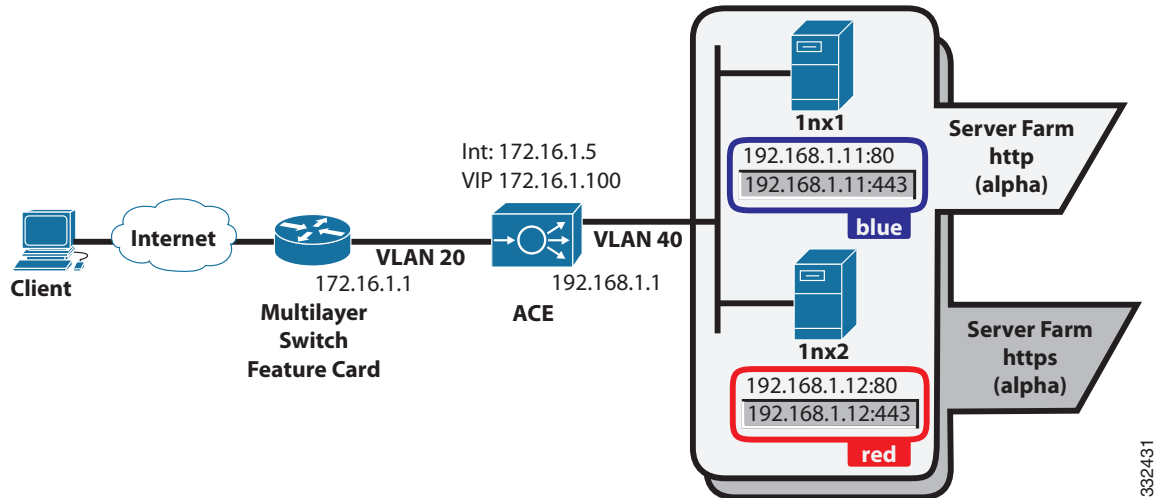
- When two sticky groups with different timeout values are buddied together, the ACE uses the shortest timeout value for the buddy group.
- Sticky groups that are buddied together must be of the same type, such as all IP-sticky, all http-cookie, and so forth. The ACE does not support different types of sticky groups buddied together.
- When two sticky groups are buddied together and one of them is configured for timeout active connections, the member group is also configured for timeout active connections.
- When two sticky groups are configured with different IP netmask (IPv4) or prefix-length (IPv6), the ACE uses the one with the most granular netmask or prefix-length.
- When a static entry is created under a buddy sticky group, its behavior is unchanged and it sticks to the same real server configured regardless of the buddy group that real server is associated with.
- Before you can configure a sticky group as a member, you must have a server farm configured under that sticky group and all the real servers that belong to that server farm have buddy group configured under them. This requirement prevents invalid configurations.
- The ACE does not support configuring the following types of sticky groups as buddy sticky group members:
  - SSL
  - RTSP Header
- The ACE supports PTMP sticky group such as SIP sticky; however, you must make sure that the configuration is the same across both sticky groups for the buddy sticky group feature to work.
- For real server backup applications:
  - We recommend only one level of backup-rserver with buddy sticky.
  - If you add a buddy group to the primary real server, the backup server inherits this buddy group. However, if you remove the buddy group from the primary real server, the buddy group is not removed from the backup real server and vice versa.

## One-to-One Association Example

In a one-to-one buddy sticky group association, you create a buddy sticky group that sticks a client to the same physical server instances in two different server farms. In the network example shown in [Figure 7-1](#), the ACE is configured with the following server farms, their associated real servers, and the buddy sticky groups that group both items:

| Server Farm                   | Server Farm<br>Buddy Member Group | Real Server           | Real Server<br>Buddy Group |
|-------------------------------|-----------------------------------|-----------------------|----------------------------|
| http<br>(for HTTP requests)   | alpha                             | 1nx1:192.168.1.11:80  | blue                       |
|                               |                                   | 1nx2:192.168.1.12:80  | red                        |
| https<br>(for HTTPS requests) | alpha                             | 1nx1:192.168.1.11:443 | blue                       |
|                               |                                   | 1nx2:192.168.1.12:443 | red                        |

**Figure 7-1** Buddy Sticky Groups: One-to-One Association



The ACE is configured to load balance HTTP requests to server farm http using either real server 1nx1:192.168.1.11:80 or 1nx2:192.168.1.12:80. The ACE is also configured to load balance HTTPS requests using server farm https and either real server 1nx1:192.168.1.11:443 or 1nx2:192.168.1.12:443. The buddy groups allow the ACE to stick a client to the same real server (for example, 1nx1) while building a shopping cart using HTTP requests and then checking out using HTTPS.

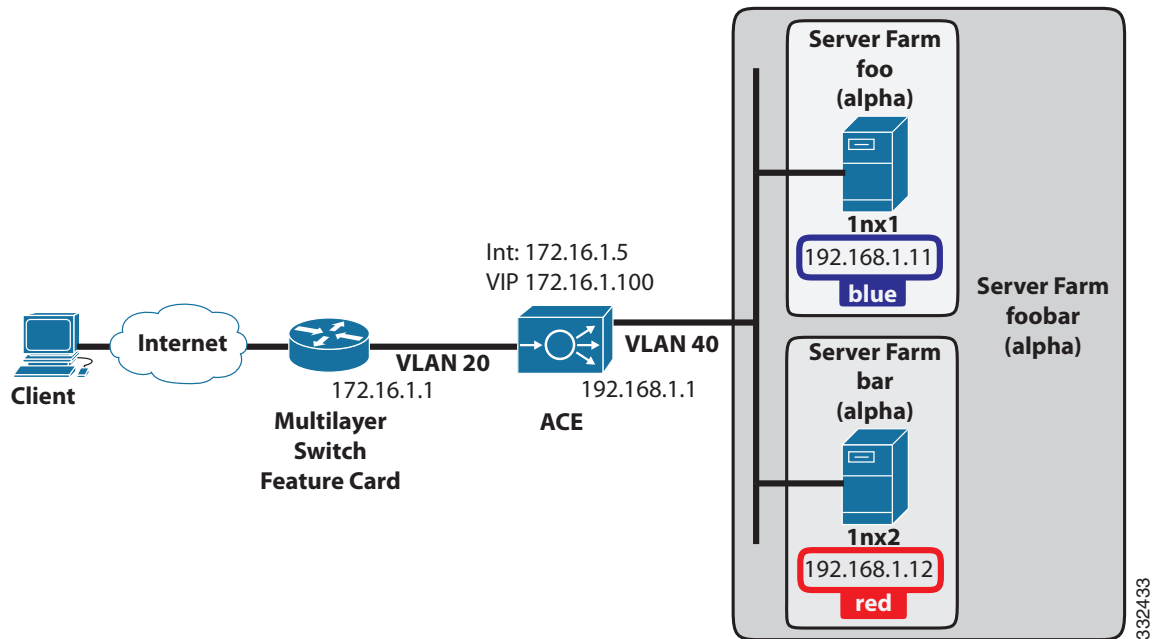
In this example, the client hits VIP 172.16.1.100, destination port 80 with an HTTP request to begin to build a shopping cart. The ACE load balances the request to server farm http, real server 1nx1:192.168.1.11:80 and creates a sticky entry based on the corresponding sticky group (for example, source IP address) that sticks the client to the real server while the client builds their shopping cart. When the client moves to the secured connection (port 443) for checkout, it hits the VIP with destination port 443 and the ACE sends the client to server farm https. The ACE finds an existing sticky entry with real server 1nx1:192.168.1.11:80 and directs the client to 1nx1:192.168.1.11:443 because the two real servers are buddied together under the blue buddy group.

## Asymmetric Association Example

In an asymmetric buddy sticky group association, you create a buddy sticky group that sticks all Layer 7 traffic from a client to a specific real server even when some of the traffic does not match the Layer 7 class map. In the network example shown in [Figure 7-2](#), the ACE is configured to include the following server farms, their associated real servers, and real server buddy sticky groups.

| Server Farm | Server Farm Buddy Member Group | Real Server | Real Server Buddy Group |
|-------------|--------------------------------|-------------|-------------------------|
| foo bar     | alpha                          | 1nx1        | blue                    |
|             |                                | 1nx2        | red                     |
| foo         | alpha                          | 1nx1        | blue                    |
| bar         | alpha                          | 1nx2        | red                     |

Figure 7-2 Buddy Sticky Groups: Asymmetric Association



The ACE is configured to send client traffic with Layer 3 matches to server farm foobar, which contains the nested server farms foo and bar. The ACE load balances the client traffic to one of the nested server farms based on Layer 7 class map matches. By defining buddy sticky groups, the ACE is also able to stick non-matching client traffic to the same real server.

In this example, the client sends traffic with Layer 3 matches that the ACE directs and sticks (using ip sticky) to server farm foobar. The ACE uses a Layer 7 class map to check for HTTP URL and if present, sends the traffic to server farm foo and sticks the client traffic to that server using sticky that is based on the source IP address. Using a buddy stick group, the ACE uses the sticky entry to send any other traffic type from the client to the same real server. For example, if the ACE sticks the client HTTP traffic to server farm foo:real server 1nx1 based on a Layer 7 class map match, the buddy stick group allows the ACE to send non-HTTP traffic from the client to the same real server.

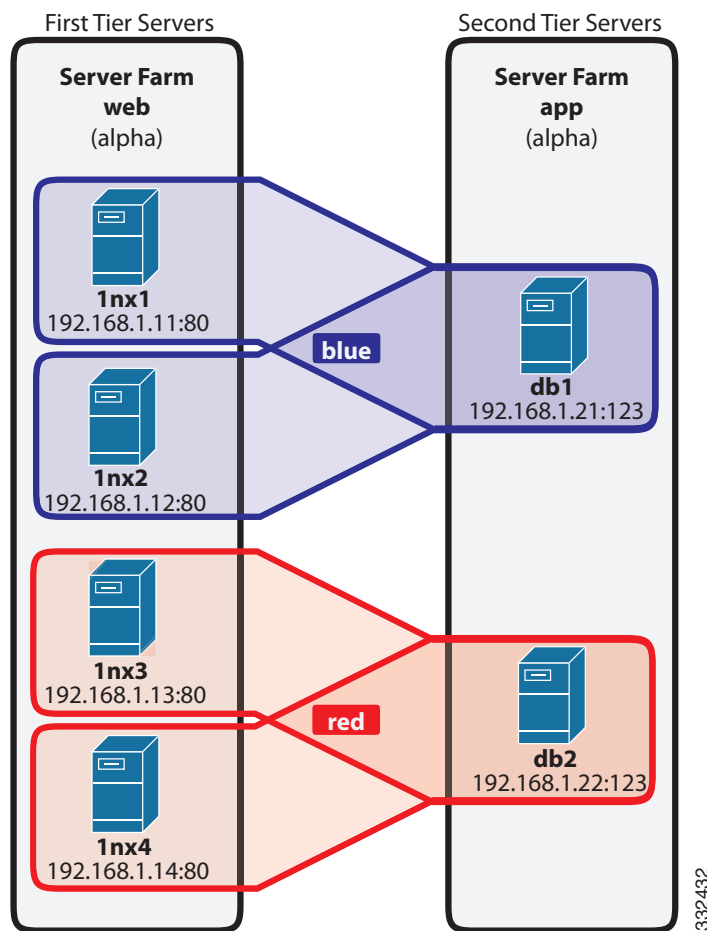
## Many-to-One Association Example

In a many-to-one buddy sticky group association, you create a buddy sticky group that sticks a group of real servers to a specific real server, which is useful when clients are load balanced to a first-tier server farm containing many real servers and are then directed to a second tier server farm that contains fewer real servers. In this type of application, you create buddy sticky groups that stick each first-tier real server group to a specific second-tier real server.

In the network example shown in [Figure 7-3](#), the ACE is configured with the following server farms, their associated real servers, and assigned real server buddy groups:

| Server Farm       | Server Farm Buddy Member Group | Real Server          | Real Server Buddy Group |
|-------------------|--------------------------------|----------------------|-------------------------|
| web (first tier)  | alpha                          | 1nx1:192.168.1.11:80 | blue                    |
|                   |                                | 1nx2:192.168.1.12:80 | blue                    |
|                   |                                | 1nx3:192.168.1.13:80 | red                     |
|                   |                                | 1nx4:192.168.1.14:80 | red                     |
| app (second tier) | alpha                          | db1:192.168.1.21:123 | blue                    |
|                   |                                | db1:192.168.1.22:123 | red                     |

**Figure 7-3** Buddy Sticky Groups: Many-to-One Association



The buddy sticky groups blue and red divide the first-tier real servers into groups and then sticks each of these groups to a specific second-tier real server.

In this example, when the ACE load balances clients to either real server 1nx1 or 1nx2 in the server farm web, the clients are directed only to real server db1 when they are ready to move to the server farm app. Notice also that clients that the ACE load balances to 1nx3 and 1nx4 are directed only to real server db2 when they are ready to move to the server farm app.

## Sticky Table

To keep track of sticky connections, the ACE appliance uses a sticky table. Table entries include the following items:

- Sticky groups
- Sticky methods
- Sticky connections
- Real servers

The sticky table can hold a maximum of four million entries (four million simultaneous users). When the table reaches the maximum number of entries, additional sticky connections cause the table to wrap and the first users become unstuck from their respective servers.

The ACE appliance uses a configurable timeout mechanism to age out sticky table entries. When an entry times out, it becomes eligible for reuse. High connection rates may cause the premature aging out of sticky entries. In this case, the ACE appliance reuses the entries that are closest to expiration first.

Sticky entries can be either dynamic (generated by the ACE appliance on-the-fly) or static (user-configured). When you create a static sticky entry, the ACE appliance places the entry in the sticky table immediately. Static entries remain in the sticky database until you remove them from the configuration. You can create a maximum of 4096 static sticky entries in each context.

If the ACE appliance takes a real server out of service for whatever reason (probe failure, no inservice command, or ARP timeout), the ACE appliance removes from the database any sticky entries that are related to that server.

### Related Topics

- [Configuring Sticky Groups, page 7-11](#)
- [Sticky Types, page 7-2](#)
- [Sticky Table, page 7-11](#)

## Configuring Sticky Groups

Stickiness (or session persistence) is a feature that allows the same client to maintain multiple simultaneous or subsequent TCP connections with the same real server for the duration of a session. A session, as used here, is defined as a series of transactions between a client and a server over some finite period of time (from several minutes to several hours). This feature is particularly useful for e-commerce applications where a client needs to maintain multiple TCP connections with the same server while shopping online, especially while building a shopping cart and during the checkout process.

E-commerce applications are not the only types of applications that require stickiness. Any Web application that maintains client information may require stickiness, such as banking applications or online trading. Other uses include FTP and HTTP file transfers.

The ACE appliance uses the concept of sticky groups to configure stickiness. A sticky group allows you to specify sticky attributes. After you configure a sticky group and its attributes, you associate the sticky group with a Layer 7 policy-map action in a Layer 7 SLB policy map.

**Procedure**

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Stickiness**. The Sticky Groups table appears.
- Step 2** Click **Add** to add a new sticky group, or select an existing sticky group you want to modify, and then click **Edit**.
- Step 3** Enter the sticky group attributes (see [Table 7-1](#)).

**Table 7-1** *Sticky Group Attributes*

| Field      | Description                                                                                                                      |
|------------|----------------------------------------------------------------------------------------------------------------------------------|
| Group Name | The sticky group identifier. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. |

Table 7-1 Sticky Group Attributes (continued)


| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type        | <p>The method to be used when establishing sticky connections:</p> <ul style="list-style-type: none"> <li>• HTTP Content—The ACE sticks client connections to the same real server based on a string in the data portion of the HTTP packet. See <a href="#">Table 7-2</a> for additional configuration options.</li> <li>• HTTP Cookie—Indicates that the ACE appliance is either to learn a cookie from the HTTP header of a client request or to insert a cookie in the Set-Cookie header of the response from the server to the client, and then use the learned cookie to provide stickiness between the client and server for the duration of the transaction.</li> <li>• HTTP Header—Indicates that the ACE appliance is to stick client connections to the same real server based on HTTP headers.</li> <li>• IP Netmask—Indicates that the ACE appliance is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both based on their IP netmask. You can optionally configure an IPv6 prefix length with this sticky type.</li> </ul> <p><b>Note</b> If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence.</p> <ul style="list-style-type: none"> <li>• IPv6 Prefix—Indicates that the ACE appliance is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both based on their IPv6 prefix. You can optionally configure an IPv4 netmask with this sticky type.</li> <li>• Layer 4 Payload—The ACE sticks client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. See <a href="#">Table 7-6</a> for additional configuration options.</li> <li>• RADIUS—The ACE sticks client connections to the same real server based on a RADIUS attribute. See <a href="#">Table 7-7</a> for additional configuration options.</li> <li>• RTSP Header—The ACE sticks client connections to the same real server based on the RTSP Session header field. See <a href="#">Table 7-8</a> for additional configuration options.</li> <li>• SIP Header—The ACE sticks client connections to the same real server based on the SIP Call-ID header field.</li> <li>• SSL—The ACE sticks client connections to the same real server based on the SSL session ID.</li> </ul> <p> <b>Note</b> This option is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> |
| Cookie Name | <p>This option appears for sticky type HTTP Cookie.</p> <p>Enter a unique identifier for the cookie. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 7-1 Sticky Group Attributes (continued)

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Insert      | <p>This option appears only for sticky type HTTP Cookie.</p> <p>Check this check box if the ACE appliance is to insert a cookie in the Set-Cookie header of the response from the server to the client. This option is useful when you want to use a session cookie for persistence but the server is not currently setting the appropriate cookie. When selected, the ACE appliance selects a cookie value that identifies the original server from which the client received a response. For subsequent connections of the same transaction, the client uses the cookie to stick to the same server.</p> <p>Clear this check box to disable cookie insertion.</p> |
| Browser Expire     | <p>This option appears for sticky type HTTP Cookie and you select Enable Insert.</p> <p>Check this check box to allow the client's browser to expire a cookie when the session ends. Clear this check box to disable browser expire.</p>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Offset (Bytes)     | <p>This option appears for sticky types HTTP Cookie and HTTP Header.</p> <p>Enter the number of bytes the ACE appliance is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the ACE appliance does not exclude any portion of the cookie.</p>                                                                                                                                                                                                                                                                                                                          |
| Length (Bytes)     | <p>This option appears for sticky types HTTP Cookie, HTTP Header, and SSL.</p> <p>Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE appliance is to use for sticking the client to the server. For the SSL sticky type, enter the SSL session ID length that needs to be parsed. Valid entries are integers from 1 to 1000.</p>                                                                                                                                                                                                                                                                            |
| Secondary Name     | <p>This option appears only for sticky type HTTP Cookie.</p> <p>Enter an alternate cookie name that is to appear in the URL string of the Web page on the server. The ACE appliance uses this cookie to maintain a sticky connection between a client and a server and adds a secondary entry in the sticky table. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</p>                                                                                                                                                                                                                                                       |
| Header Name        | <p>This option appears for sticky type HTTP Header.</p> <p>Select the HTTP header to use for sticking client connections.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IPv4 Netmask       | <p>This option appears only for sticky type IP Netmask or IPv6 Prefix. This option is mandatory for the sticky type IP Netmask and optional for the sticky type IPv6 Prefix.</p> <p>Select the netmask to apply to the source IP address, the destination IP address, or both.</p>                                                                                                                                                                                                                                                                                                                                                                                  |
| IPv6 Prefix Length | <p>This option appears only for sticky type IPv6 Prefix or IP Netmask. This option is mandatory for the sticky type IPv Prefix and optional for the sticky type IP Netmask.</p> <p>Enter the IPv6 prefix length to apply to the source IP address, the destination IP address, or both.</p>                                                                                                                                                                                                                                                                                                                                                                         |
| Address Type       | <p>This option appears only for sticky type IP Netmask or IPv6 Prefix.</p> <p>Indicate whether this sticky type is to be applied to the client source IP address, the destination IP address, or both:</p> <ul style="list-style-type: none"> <li>Both—Indicates that this sticky type is to be applied to both the source IP address and the destination IP address.</li> <li>Destination—Indicates that this sticky type is to be applied to the destination IP address only.</li> <li>Source—Indicates that this sticky type is to be applied to the source IP address only.</li> </ul>                                                                          |



Table 7-1 Sticky Group Attributes (continued)

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Sticky For Response          | This check box option appears for sticky types: Layer 4 Payload and SSL.<br>Check this check box to instruct the ACE to parse the response bytes from a server and perform sticky learning. Clear the check box when you do not want the ACE to perform this operation.                                                                                                                                                                                                                                                           |
| Sticky Server Farm                  | Select a server farm you want to associate with this sticky group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Backup Server Farm                  | This field appears when a server farm is selected.<br>Select a backup server farm to be associated with this sticky group. If the primary server farm is down, the ACE appliance uses the backup server farm.                                                                                                                                                                                                                                                                                                                     |
| Aggregate State                     | This field appears when a server farm and backup server farm are selected.<br>Check this check box to indicate that the state of the backup server farm is tied to the virtual server state. Clear this check box if the backup server farm is not tied to the virtual server state.                                                                                                                                                                                                                                              |
| Enable Sticky on Backup Server Farm | This field appears when a server farm and backup server farm are selected.<br>Check this check box to indicate that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky.                                                                                                                                                                                                                                                                                                               |
| Buddy Group                         | This field appears when a server farm is selected.<br>Associate the server farm with an existing buddy sticky group or create a buddy sticky group. When you associate multiple server farms with the same buddy group, client requests are stuck to the same real server even when the requests are processed by different server farms. For more information, see the <a href="#">“Buddy Sticky Groups” section on page 7-6</a> .<br><b>Note</b> The ACE does not support the buddy group feature for SSL or RTSP sticky types. |
| Replicate on HA Peer                | Check this check box to indicate that the ACE appliance to replicate sticky table entries on the standby ACE appliance. If a failover occurs and this option is selected, the new active ACE appliance can maintain the existing sticky connections.<br>Clear this check box to indicate that the ACE appliance is not to replicate sticky table entries on the standby ACE appliance.                                                                                                                                            |
| Timeout (Minutes)                   | Enter the number of minutes that the ACE appliance keeps the sticky information for a client connection in the sticky table after the latest client connection terminates. Valid entries are integers from 1 to 65535; the default is 1440 minutes (24 hours).                                                                                                                                                                                                                                                                    |
| Timeout Active Connections          | Check this check box to specify that the ACE appliance is to time out sticky table entries even if active connections exist after the sticky timer expires.<br>Clear this check box to specify that the ACE appliance is not to time out sticky table entries even if active connections exist after the sticky timer expires. This is the default behavior.                                                                                                                                                                      |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. To configure sticky statics, see [Configuring Sticky Statics, page 7-21](#).
- Click **Cancel** to exit the procedure without saving your entries and to return to the Sticky Groups table.
- Click **Next** to save your entries and to configure another sticky group.

**Related Topics**

- [Configuring Sticky Statics, page 7-21](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Server Farms, page 6-18](#)

## Sticky Group Attribute Tables

Refer to the following topics for sticky group type-specific attributes:

- [HTTP Content Sticky Group Attributes, page 7-16](#)
- [HTTP Cookie Sticky Group Attributes, page 7-17](#)
- [HTTP Header Sticky Group Attributes, page 7-18](#)
- [IP Netmask Sticky Group Attributes, page 7-18](#)
- [Layer 4 Payload Sticky Group Attributes, page 7-19](#)
- [RADIUS Sticky Group Attributes, page 7-20](#)
- [RTSP Header Sticky Group Attributes, page 7-20](#)
- [SSL Header Sticky Group Attributes, page 7-21](#)

### HTTP Content Sticky Group Attributes

**Table 7-2** *HTTP Content Sticky Group Attributes*

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP Content   | HTTP content may change over time with only a portion remaining constant throughout a transaction between the client and a server.<br><br>Check the check box to configure the ACE to use the constant portion of HTTP content to make persistent connections to a specific server. Clear the check box to identify specific content for stickiness in the Offset, Length, Begin Pattern, and End Pattern fields. |
| Offset (Bytes) | Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.                                                                                                                                                      |
| Length (Bytes) | Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.                                                                                                                                                                                                            |

Table 7-2 HTTP Content Sticky Group Attributes (continued)

| Field         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Begin Pattern | <p>Enter the beginning pattern of the HTTP content payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE begins parsing immediately after the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                               |
| End Pattern   | <p>Enter the pattern that marks the end of hashing. If you do not specify an end pattern or a length, the ACE continues to parse the data until it reaches the end of the field or packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> |

## HTTP Cookie Sticky Group Attributes

Table 7-3 HTTP Cookie Sticky Group Attributes

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cookie Name    | Enter a unique identifier for the cookie. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Enable Insert  | <p>Check the check box if the virtual server is to insert a cookie in the Set-Cookie header of the response from the server to the client. This option is useful when you want to use a session cookie for persistence but the server is not currently setting the appropriate cookie. When selected, the virtual server selects a cookie value that identifies the original server from which the client received a response. For subsequent connections of the same transaction, the client uses the cookie to stick to the same server.</p> <p>Clear the check box to disable cookie insertion.</p> |
| Browser Expire | <p>This option appears for sticky type HTTP Cookie and you select Enable Insert.</p> <p>Check this check box to allow the client's browser to expire a cookie when the session ends. Clear this check box to disable browser expire.</p>                                                                                                                                                                                                                                                                                                                                                               |
| Offset (Bytes) | Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.                                                                                                                                                                                                                                                                                                                                           |

**Table 7-3** *HTTP Cookie Sticky Group Attributes (continued)*

| Field          | Description                                                                                                                                                                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Length (Bytes) | Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.                                                                                                                                     |
| Secondary Name | Enter an alternate cookie name that is to appear in the URL string of the Web page on the server. The virtual server uses this cookie to maintain a sticky connection between a client and a server and adds a secondary entry in the sticky table. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. |

### HTTP Header Sticky Group Attributes

**Table 7-4** *HTTP Header Sticky Group Attributes*

| Field          | Description                                                                                                                                                                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Header Name    | Select the HTTP header to use for sticking client connections.                                                                                                                                                                                               |
| Offset (Bytes) | Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie. |
| Length (Bytes) | Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.                                                       |

### IP Netmask Sticky Group Attributes

**Table 7-5** *IP Netmask Sticky Group Attributes*

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Netmask      | Select the netmask to apply to the source IP address, destination IP address, or both.                                                                                                                                                                                                                                                                                                                                                                   |
| Address Type | Indicate whether this sticky type is to be applied to the client source IP address, the destination IP address, or both: <ul style="list-style-type: none"> <li>Both—The sticky type is to be applied to both the source IP address and the destination IP address.</li> <li>Destination—The sticky type is to be applied to the destination IP address only.</li> <li>Source—The sticky type is to be applied to the source IP address only.</li> </ul> |

## Layer 4 Payload Sticky Group Attributes

**Table 7-6** *Layer 4 Payload Sticky Group Attributes*

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Offset (Bytes)             | Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Length (Bytes)             | Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Begin Pattern              | <p>Enter the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE begins parsing immediately after the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                                    |
| End Pattern                | <p>Enter the pattern that marks the end of hashing. If you do not specify an end pattern or a length, the ACE continues to parse the data until it reaches the end of the field or packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> |
| Enable Sticky For Response | <p>Check the check box to enable the ACE to parse server responses and perform sticky learning. The ACE uses a hash of the server response bytes to populate the sticky database. The next time that the ACE receives a client request with those same bytes, it sticks the client to the same server.</p> <p>Clear the check box to reset the behavior of the ACE to the default of not parsing server responses and performing sticky learning.</p>                                                                                                                                                                                                                                                                                                                                                  |

## RADIUS Sticky Group Attributes

**Table 7-7** *RADIUS Sticky Group Attributes*

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS Types                 | <p>Select the RADIUS attribute to use for sticking client connections:</p> <ul style="list-style-type: none"> <li>N/A—This option is not configured.</li> <li>RADIUS Calling ID—Stickiness is based on the RADIUS framed IP attribute and the calling station ID attribute.</li> <li>RADIUS User Name—Stickiness is based on the RADIUS framed IP attribute and the username attribute.</li> </ul>                                   |
| Enter User IPv6Prefix Length | <p>Enter the IPv6 prefix length for IPv6 end user packets when using RADIUS IPv6 attributes. For RADIUS-framed IP sticky using IPv6, the sticky entry is based on the framed IPv6 prefix and prefix length in the RADIUS packet. Use a matching prefix length for the sticky lookup of end user packets.</p> <p>Enter a prefix length from 1 to 128. The default is 64.</p>                                                          |
| Wait For Acknowledgement     | <p>Check this check box to configure the ACE to reload-balance RADIUS requests that hit framed-ip sticky entries (excluding the real server in sticky entry) when the Accounting-Start does not receive a response. This feature is designed for scenarios in which sticky entries are created during the Accounting phase.</p> <p>Clear this check box to configure the ACE not to use the wait for an acknowledgement feature.</p> |
| Radius Purge Information     | <p>When the user chooses the <b>TYPE</b> option as <b>RADIUS</b> in the drop down, Radius Purge Information checkbox is displayed.</p>                                                                                                                                                                                                                                                                                               |

## RTSP Header Sticky Group Attributes

**Table 7-8** *RTSP Header Sticky Group Attributes*

| Field          | Description                                                                                                                                                                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Offset (Bytes) | <p>Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.</p> |
| Length (Bytes) | <p>Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.</p>                                                       |

## SSL Header Sticky Group Attributes

Table 7-9 *SSL Sticky Group Attributes*

| Field                      | Description                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Sticky For Response | Check the check box to instruct the ACE to parse the response bytes from a server and perform sticky learning. Clear the check box when you do not want the ACE to perform this operation. |
| Length (Bytes)             | Length of the SSL session ID that needs to be parsed. Valid entries are integers from 1 to 1000.                                                                                           |

## Viewing All Sticky Groups by Context

Use this procedure to view all sticky groups associated with a virtual context.

### Procedure

- Step 1** Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.
- Step 2** Select the virtual context with the sticky groups you want to view, and then select **Load Balancing > Stickiness**. The Sticky Groups table appears, listing the sticky groups associated with the selected context.

### Related Topics

- [Configuring Sticky Groups, page 7-11](#)
- [Configuring Sticky Statics, page 7-21](#)

## Configuring Sticky Statics

Use this procedure to configure sticky statics.

### Assumption

A sticky group has been configured. See [Configuring Sticky Groups, page 7-11](#) for more information.

### Procedure

- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Stickiness**. The Sticky Groups table appears.
- Step 2** Select the sticky group you want to configure for sticky statics, and then select the Sticky Statics tab. If you do not see the Sticky Statics tab beneath the Sticky Groups table, click the **Switch between Configure and Browse Modes** button.
- Step 3** Click **Add** to add a new entry to the table, or select an existing entry, and then click **Edit** to modify it. The Sticky Statics configuration screen appears.

- Step 4** In the Sequence Number field, either accept the automatically incremented number for this entry or enter a new sequence number. The sequence number indicates the order in which multiple sticky static configurations are applied.
- Step 5** In the Type field, confirm that the correct sticky group type is selected. If you select multiple sticky groups and are creating a new static sticky entry, select the sticky group type to use as shown in [Table 7-10](#).

**Table 7-10**      *Sticky Group Types*

| Sticky Group    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP Content    | Indicates that the ACE appliance is to stick a client to a server based on the content of an HTTP packet. You can specify a beginning pattern and ending pattern, the number of bytes to parse, and an offset that specifies how many bytes to ignore from the beginning of the data.                                                                                                                                                                                                                                                                                                                                                                                                |
| HTTP Cookie     | Indicates that the ACE appliance is either to learn a cookie from the HTTP header of a client request or to insert a cookie in the Set-Cookie header of the response from the server to the client, and then use the learned cookie to provide stickiness between the client and server for the duration of the transaction.                                                                                                                                                                                                                                                                                                                                                         |
| HTTP Header     | Indicates that the ACE appliance is to stick client connections to the same real server based on HTTP headers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IP Netmask      | Indicates that the ACE appliance is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both based on the IPv4 netmask. You can optionally configure an IPv6 prefix length with this sticky type.<br><br><b>Note</b> If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence. |
| IPv6 Prefix     | Indicates that the ACE appliance is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both based on the IPv6 prefix length. You can optionally configure an IPv4 netmask with this sticky type.                                                                                                                                                                                                                                                                                                                                                        |
| Layer 4 Payload | Indicates that the ACE appliance is to stick a client to a server based on the data in Layer 4 frames. You can specify a beginning pattern and ending pattern, the number of bytes to parse, and an offset that specifies how many bytes to ignore from the beginning of the data.                                                                                                                                                                                                                                                                                                                                                                                                   |
| RADIUS          | Indicates that the ACE appliance is to stick client connections based on the following RADIUS attributes: Calling station ID or Username.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| RTSP Header     | Indicates that the ACE appliance is to stick client connections based on information in the RTSP session header. With RTSP header stickiness, you can specify a header offset to provide stickiness based on a unique portion of the RTSP header.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SIP Header      | Indicates that the ACE appliance is to stick client connections based on the SIP Call-ID header field. SIP header stickiness requires the entire SIP header, so you cannot specify an offset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



- Step 6** If you select either HTTP Cookie, HTTP Header, HTTP Content, Layer 4 Payload, RTSP header, or SIP header for sticky type, in the Static Value field, enter the cookie string value. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters. If the string includes spaces, enclose the string with quotes.
- Step 7** If you select IP Netmask or IPv6 Prefix for the sticky type:
- For the IP Address Type, select either IPv4 or IPv6.
  - In the Static Source field, enter the source IP address of the client.
  - In the Static Destination field, enter the destination IP address of the client.
- Step 8** In the Named Real Server field, select the real server to associate with this static sticky entry.
- Step 9** In the Port field, enter the port number of the real server. Valid entries are integers from 1 to 65535.
- Step 10** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Sticky Statics table.
  - Click **Next** to save your entries and to configure another sticky static entry.
- 

**Related Topic**

[Configuring Sticky Groups, page 7-11](#)





## CHAPTER 8

# Configuring Parameter Maps

This chapter describes how to configure parameter maps. Parameter maps provide a means of performing actions on traffic received by the ACE, based on certain criteria such as protocol or connection attributes. After you configure a parameter map, you associate it with a policy map to implement configured behavior.

[Table 8-1](#) describes the parameter maps you can configure using the ACE.

**Table 8-1** *Parameter Map Types*

| Parameter Map | Description                                                                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection    | Connection parameter maps combine all IP and TCP connection-related behaviors pertaining to the following: <ul style="list-style-type: none"><li>• TCP normalization, termination, and server reuse</li><li>• IP normalization, fragmentation, and reassembly</li></ul> |
| DNS           | Domain Name System (DNS) parameter maps configure DNS actions for DNS packet inspection.                                                                                                                                                                                |
| Generic       | Generic parameter maps combine related generic protocol actions for server load-balancing connections.                                                                                                                                                                  |
| HTTP          | HTTP parameter maps configure ACE behavior for HTTP load-balanced connections.                                                                                                                                                                                          |
| Optimization  | Optimization parameter maps specify optimization-related commands that pertain to application acceleration and optimization functions performed by the ACE.                                                                                                             |
| RDP           | Remote Desktop Protocol (RDP) parameter maps configure routing-token-rebalance in which the ACE redirects a connection that contains RDP packets to another server when the real server that matches the token information in the client request is down.               |
| RTSP          | RTSP parameter maps configure advanced RTSP behavior for server load-balancing connections.                                                                                                                                                                             |
| SIP           | Session Initiation Protocol (SIP) parameter maps configure SIP deep packet inspection on the ACE.                                                                                                                                                                       |
| Skinny        | Skinny Client Control Protocol (SCCP) parameter maps configure SCCP packet inspection on the ACE.                                                                                                                                                                       |



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

This chapter contains the following sections:

- [Configuring HTTP Parameter Maps, page 8-2](#)
- [Configuring Connection Parameter Maps, page 8-5](#)
- [Configuring Optimization Parameter Maps, page 8-11](#)
- [Configuring Generic Parameter Maps, page 8-17](#)
- [Configuring RTSP Parameter Maps, page 8-19](#)
- [Configuring SIP Parameter Maps, page 8-20](#)
- [Configuring Skinny Parameter Maps, page 8-22](#)
- [Configuring DNS Parameter Maps, page 8-23](#)
- [Configuring RDP Parameter Maps, page 8-24](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

## Configuring HTTP Parameter Maps

Use this procedure to configure an HTTP parameter map for use with a Layer 3/Layer 4 policy map.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > HTTP Parameter Maps**. The HTTP Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The HTTP Parameter Maps configuration screen appears.
- Step 3** In the Parameter Name field, enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 4** Enter the information in [Table 8-2](#).

**Table 8-2** HTTP Parameter Map Attributes

| Field            | Description                                                                                                                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description      | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs. |
| Case-Insensitive | Check this check box to indicate that the ACE appliance is to be case insensitive. Clear this check box to indicate that the ACE appliance is to be case sensitive. This check box is cleared by default.              |

Table 8-2 HTTP Parameter Map Attributes (continued)

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Header Modify Per-Request    | Check the check box to require SSL information be inserted for every HTTP GET request. Current functionality only requires that the information be inserted at the first GET request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Exceed Max. Parse Length     | <p>Indicate how the ACE appliance is to handle cookies, HTTP headers, and URLs that exceed the maximum parse length:</p> <ul style="list-style-type: none"> <li>Continue—Indicates that the ACE appliance is to continue load balancing. When this option is selected, the HTTP Persistence Rebalance option is disabled if the total length of all cookies, HTTP headers, and URLs exceeds the maximum parse value.</li> <li>Drop—Indicates that the ACE appliance is to stop load balancing and to discard the packet.</li> </ul>                                                                                                                                                                                                                                                                                |
| HTTP Persistence Rebalance   | <p>Check this check box to enabled persistence rebalance. Persistence is sometimes referred to as a connection keepalive.</p> <p>With persistence rebalance enabled, when successive GET requests result in load balancing that chooses the same policy, the ACE sends the request to the real server used for the last GET request. This behavior prevents the ACE from load balancing every request and recreating the server-side connection on every GET request, producing less overhead and better performance.</p> <p>Another effect of persistence rebalance is that header insertion and cookie insertion, if enabled, occur for every request instead of only the first request.</p> <p>By default, persistence rebalance is enabled. Clear this check box to indicate that this option is disabled.</p> |
| TCP Server Connection Reuse  | <p>Check this check box to indicate that the ACE appliance is to reduce the number of open connections on a server by allowing connections to persist and be reused by multiple client connections. If you enable this feature:</p> <ul style="list-style-type: none"> <li>Ensure that the ACE appliance maximum segment size (MSS) is the same as the server maximum segment size.</li> <li>Configure port address translation (PAT) on the interface that is connected to the real server.</li> <li>Configure on the ACE appliance the same TCP options that exist on the TCP server.</li> <li>Ensure that each server farm is homogeneous (all real servers within a server farm have identical configurations).</li> </ul> <p>Clear this check box to disable this option.</p>                                 |
| Enable Drop on Parsing Error | <p>Check this check box to have the ACE drop a connection when it detects a parse error.</p> <p>Clear the check box to disable this option and configure the ACE maintain a connection even when it detects a parse error. This is the default setting.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Table 8-2 HTTP Parameter Map Attributes (continued)

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Non Strict on Parsing Error | <p>Check this check box to configure the ACE to allow the presence of a CRLF in the header before the header name, which is inserted for header name continuation purposes. Normally, the ACE considers a CRLF in the header a parse error. When you enable this feature and the ACE encounters a CRLF in the header, the ACE ignores the parse error and allows the Layer 7 connection.</p> <p>Clear the check box to disable this feature and configure the ACE to not allow a CRLF in the header. When the ACE encounters a CRLF, it considers it a parsing error and reacts according to how you set the <a href="#">Enable Drop on Parsing Error</a> field. This is the default setting.</p>                                                                                                                                                                                                                           |
| Content Max. Parse Length (Bytes)  | Enter the maximum number of bytes to parse in HTTP content. Valid entries are integers from 1 to 65535, with a default of 4096.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Header Max. Parse Length (Bytes)   | Enter the maximum number of bytes to parse for the total length of cookies, HTTP headers, and URLs. Valid entries are integers from 1 to 65535 with a default of 4096.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Secondary Cookie Delimiters        | Enter the ASCII-character delimiters to be used to separate cookies in a URL string. Valid entries are unquoted text strings with no spaces and a maximum of 4 characters. The default delimiters are /&#+.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| MIME Type To Compress              | <p>In the field on the left, enter the Multipurpose Internet Mail Extension (MIME) type to compress, and then click <b>Add</b>. The MIME type appears in the column on the right. To remove or change a MIME type, select it in the column on the right, and then click <b>Remove</b>. The selected MIME type appears in the field on the left where you can modify or delete it.</p> <p>To specify the sequence in which compression is to be applied, select MIME types in the column on the right, and then click <b>Up</b> or <b>Down</b> to arrange the MIME types.</p> <p><a href="#">Supported MIME Types, page 8-25</a> lists the supported MIME types. You can use an asterisk (*) to indicate a wildcard, such as <code>text/*</code>, which would include all text MIME types (text/html, text/plain, and so on).</p>                                                                                            |
| User Agent Not To Compress         | <p>A user agent is a client that initiates a request. Examples of user agents include browsers, editors, and other end-user tools. When you specify a user agent string in this field, the ACE appliance does not compress the response to a request when the request contains the matching user agent string.</p> <p>In the field on the left, enter the user agent string to be matched, and then click <b>Add</b>. The string appears in the column on the right. To remove or change a user agent string, select it in the column on the right, and then click <b>Remove</b>. The selected string appears in the field on the left where you can modify or delete it.</p> <p>To specify the sequence in which strings are to be matched, select strings in the column on the right, and then click <b>Up</b> or <b>Down</b> to arrange the strings in the desired sequence.</p> <p>Valid entries are 64 characters.</p> |
| Min. Size To Compress (Bytes)      | Enter the threshold at which compression is to occur. The ACE appliance compresses files that are the minimum size or larger. Valid entries are integers from 1 to 4096 bytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Maps table.

- Click **Next** to accept your entries and to add another parameter map.

#### Related Topics

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Optimization Parameter Maps, page 8-11](#)
- [Configuring Virtual Contexts, page 4-1](#)

## Configuring Connection Parameter Maps

Connection parameter maps combine all IP and TCP connection-related behaviors that pertain to the following:

- TCP normalization, termination, and server reuse
- IP normalization, fragmentation, and reassembly

Use this procedure to configure a Connection parameter map for use with a Layer 3/Layer 4 policy map.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > Connection Parameter Maps**. The Connection Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The Connection Parameter Maps configuration screen appears.
- Step 3** In the Parameter Name field, enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 4** Enter the information in [Table 8-3](#). Click **More Settings** to access the additional Connection Parameter Map configuration attributes. By default, ACE appliance Device Manager hides the default Connection Parameter Map configuration attributes and the attributes which are not commonly used.

**Table 8-3** *Connection Parameter Map Attributes*

| Field                        | Description                                                                                                                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter Name               | Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                  |
| Description                  | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Enter double quotes as matching pairs.    |
| Inactivity Timeout (Seconds) | Enter the number of seconds that the ACE is to wait before disconnecting idle connections. Valid entries are integers from 0 to 3217203. A value of 0 indicates that ACE is never to time out a TCP connection. |

Table 8-3 Connection Parameter Map Attributes (continued)

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Settings</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Exceeds MSS                   | <p>Indicate how the ACE is to handle segments that exceed the maximum segment size (MSS):</p> <ul style="list-style-type: none"> <li>• Allow—The ACE is to permit segments that exceed the configured MSS.</li> <li>• Drop—The ACE is to discard segments that exceed the configured MSS.</li> </ul>                                                                                                                                                                                                        |
| Full Proxy MSS Mismatch       | Allows the ACE to splice together the client front-end and the server back-end connections when the ACE is proxying Layer 7 traffic flow and the negotiated front-end and back-end TCP handshakes do not match. Uncheck the check box when you do not want the ACE to enable a connection when the TCP handshakes do not match.                                                                                                                                                                             |
| Max. Connection Limit         | Enter the maximum number of concurrent connections to allow for the parameter map. Valid entries are integers from 0 to 4000000.                                                                                                                                                                                                                                                                                                                                                                            |
| Nagle                         | <p>The Nagle algorithm instructs a sender to buffer any data to be sent until all outstanding data has been acknowledged or until there is a full segment of data to send. Enabling the Nagle algorithm increases throughput, but it can increase latency in your TCP connection.</p> <p>Check the check box to enable the Nagle algorithm. Clear the check box to disable the Nagle algorithm.</p> <p><b>Note</b> Disable the Nagle algorithm when you observe unacceptable delays in TCP connections.</p> |
| Random Sequence Number        | <p>Randomizing TCP sequence numbers adds a measure of security to TCP connections by making it more difficult for a hacker to guess or predict the next sequence number in a TCP connection.</p> <p>Check the check box to enable the use of random TCP sequence numbers. Clear the check box to disable the use of random TCP sequence numbers.</p> <p>This option is enabled by default.</p>                                                                                                              |
| Bandwidth Rate Limit          | Enter the bandwidth-rate limit in bytes per second for the parameter map. Valid entries are integers from 0 to 300000000 bytes.                                                                                                                                                                                                                                                                                                                                                                             |
| Connection Rate Limit         | Enter the connection-rate limit in connections per second. Valid entries are integers from 0 to 350000.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Reserved Bits                 | <p>Indicate how the ACE is to handle segments with the reserved bits set in the TCP header:</p> <ul style="list-style-type: none"> <li>• Allow—Segments with the reserved bits are to be permitted.</li> <li>• Drop—Segments with the reserved bits are to be discarded.</li> <li>• Clear—Reserved bits in TCP headers are to be cleared and segments are to be allowed.</li> </ul>                                                                                                                         |
| Type-of-Service IP Header     | <p>The type of service for an IP packet determines how the network handles the packet and balances its precedence, throughput, delay, reliability, and cost.</p> <p>Enter the type-of-service value to be applied to IP packets. Valid entries are integers from 0 to 255.</p> <p>For more information about type of service, refer to RFCs 791, 1122, 1349, and 3168.</p>                                                                                                                                  |
| ACK Delay Time (Milliseconds) | Enter the number of milliseconds that the ACE is to wait before sending an acknowledgement from a client to a server. Valid entries are integers from 0 to 400.                                                                                                                                                                                                                                                                                                                                             |



Table 8-3 Connection Parameter Map Attributes (continued)

| Field                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCP Buffer Share (Bytes)                    | <p>To improve throughput and overall performance, the ACE buffers the number of bytes you specify before processing received data or transmitting data. Use this option to increase the default buffer size and thereby realize improved network performance.</p> <p>Enter the maximum size of the TCP buffer in bytes. Valid entries are integers from 8192 to 262143 bytes. Default is 32768.</p> <p><b>Note</b> If you enter a value in this field for an ACE device that does not support this option, an error message appears. Leave this field blank when creating or modifying a connection parameter map for devices that do not support this option.</p>                                                                                                                                                                                                                                                                                                                                                            |
| TCP Buffer Threshold (%)                    | <p>Select the TCP buffer threshold, expressed as a percent, to indicate when the TCP connection is to be reset. This entry represents the maximum number of TCP connections that the hosts can open. This entry prevents the ACE from exhausting all available buffers due to the outage caused by DDoS attack.</p> <p>The options are 50, 75, 77, 88, 95, and 100. The default value is 100.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Smallest TCP MSS (Bytes)                    | Enter the size of the smallest segment of TCP data that the ACE is to accept. Valid entries are integers from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a minimum limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Largest TCP MSS (Bytes)                     | Enter the size of the largest segment of TCP data that the ACE is to accept. Valid entries are integers from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a maximum limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SYN Retries                                 | Enter the number of attempts that the ACE is to make to transmit a TCP segment when initiating a Layer 7 connection. Valid entries are integers from 1 to 15 with a default of 4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| TCP WAN Optimization RTT                    | <p>This option specifies how the ACE is to apply TCP optimizations to packets on a connection associated with a Layer 7 policy map using a round-trip time (RTT) value:</p> <ul style="list-style-type: none"> <li>An entry of <b>0</b> (zero) indicates that the ACE is to apply TCP optimizations to packets for the life of a connection.</li> <li>An entry of <b>65535</b> (the default) indicates that the ACE is to perform normal operations (that is, without optimizations) for the life of a connection.</li> <li>Entries from 1 to 65534 indicate that the ACE is to use the following guidelines: <ul style="list-style-type: none"> <li>If the actual client RTT is less than the configured RTT, the ACE performs normal operations for the life of the connection.</li> <li>If the actual client RTT is greater than or equal to the configured RTT, the ACE performs TCP optimizations on the packets for the life of a connection.</li> </ul> </li> </ul> <p>Valid entries are integers from 0 to 65535.</p> |
| Timeout For Embryonic Connections (Seconds) | <p>An embryonic connection is a TCP three-way handshake for a connection that does not complete for some reason.</p> <p>Enter the number of seconds that the ACE is to wait before timing out an embryonic connection. Valid entries are integers from 0 to 4294967295 with a default of 5. A value of 0 indicates that the ACE is never to time out an embryonic connection.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Half Closed Timeout (Seconds)               | <p>A half-closed connection is one in which the client or server sends a FIN and the server or client acknowledges the FIN without sending a FIN itself.</p> <p>Enter the number of seconds the ACE is to wait before closing a half-closed connection. Valid entries are integers from 0 to 4294967295 with a default of 3600 (1 hour). A value of 0 indicates that the ACE is never to time out a half-closed connection.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 8-3 Connection Parameter Map Attributes (continued)

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Slow Start Algorithm         | <p>When enabled, the slow start algorithm increases the TCP window size as ACK handshakes arrive so that new segments are injected into the network at the rate at which acknowledgements are returned by the host at the other end of the connection.</p> <p>Check this check box to enable the slow start algorithm, and clear this check box to disable the slow start algorithm. This option is disabled by default.</p>                                                                                                             |
| SYN Segments With Data       | <p>Indicate how the ACE is to handle TCP SYN segments that contain data:</p> <ul style="list-style-type: none"> <li>Allow—The ACE is to permit SYN segments that contain data and mark them for processing.</li> <li>Drop—The ACE is to discard SYN segments that contain data.</li> </ul>                                                                                                                                                                                                                                               |
| Urgent Pointer Policy        | <p>Urgent data, as indicated by a control bit in the TCP header, indicates that urgent data is to be processed as soon as possible, even before normal data.</p> <p>Indicate how the ACE is to handle urgent data as identified by the Urgent data control bit:</p> <ul style="list-style-type: none"> <li>Allow—The ACE is to permit the status of the Urgent control bit.</li> <li>Clear—The ACE is to set the Urgent control bit to 0 (zero) and thereby invalidate the Urgent Pointer which provides segment information.</li> </ul> |
| TCP Window Scale Factor      | <p>The TCP window scaling extension expands the definition of the TCP window to 32 bits and uses a scale factor to carry the 32-bit value in the 16-bit window of the TCP header. Increasing the window size improves TCP performance in network paths with large bandwidth, long-delay characteristics.</p> <p>Enter the window scale factor in this field. Valid entries are integers from 0 to 14 (the maximum scale factor).</p> <p>For more information on TCP window scaling, refer to RFC 1323.</p>                               |
| Action For TCP Options Range | <p>Indicate how the ACE is to handle the TCP options:</p> <ul style="list-style-type: none"> <li>Selective ACK</li> <li>Timestamps</li> <li>Action For TCP Window Scale Factor</li> </ul> <p>By selecting one of the options:</p> <ul style="list-style-type: none"> <li>N/A—This option is not set.</li> <li>Allow—The ACE is to allow any segment with the specified option set.</li> <li>Drop—The ACE is to discard any segment with the specified option set.</li> </ul>                                                             |
| Lower TCP Options            | <p>Appears if you select Allow or Drop for the Action For TCP Options Range.</p> <p>Enter the lower limit of the TCP option range. Valid entries are 6, 7, or an integer from 9 to 255. See <a href="#">Table 8-4</a> for information on TCP options.</p>                                                                                                                                                                                                                                                                                |
| Upper TCP Options            | <p>Appears if you select Allow or Drop for the Action For TCP Options Range.</p> <p>Enter the upper limit of the TCP option range. Valid entries are 6, 7, or an integer from 9 to 255. See <a href="#">Table 8-4</a> for information on TCP options.</p>                                                                                                                                                                                                                                                                                |
| Selective ACK                | <p>Indicate how the ACE is to handle the selective ACK option that is specified in SYN segments:</p> <ul style="list-style-type: none"> <li>Allow—The ACE is to allow any segment with the specified option set.</li> <li>Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.</li> </ul>                                                                                                                                                                                              |

Table 8-3 Connection Parameter Map Attributes (continued)

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamps                         | <p>Indicate how the ACE is to handle the timestamp option that is specified in SYN segments:</p> <ul style="list-style-type: none"> <li>Allow—The ACE is to allow any segment with the specified option set.</li> <li>Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.</li> </ul>                                                                                              |
| Action For TCP Window Scale Factor | <p>Indicate how the ACE is to handle the TCP window scale factor option that is specified in SYN segments:</p> <ul style="list-style-type: none"> <li>Allow—The ACE is to allow any segment with the specified option set.</li> <li>Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.</li> <li>Drop—The ACE is to discard any segment with the specified option set.</li> </ul> |

Table 8-4 TCP Options for Connection Parameter Maps<sup>1</sup>

| Kind | Length | Meaning                                     |
|------|--------|---------------------------------------------|
| 6    | 6      | Echo (obsoleted by option 8)                |
| 7    | 6      | Echo Reply (obsoleted by option 8)          |
| 9    | 2      | Partial Order Connection Permitted          |
| 10   | 3      | Partial Order Service Profile               |
| 11   |        | CC                                          |
| 12   |        | CC.NEW                                      |
| 13   |        | CC.ECHO                                     |
| 14   | 3      | TCP Alternate Checksum Request              |
| 15   | N      | TCP Alternate Checksum Data                 |
| 16   |        | Skeeter                                     |
| 17   |        | Bubba                                       |
| 18   | 3      | Trailer Checksum Option                     |
| 19   | 18     | MD5 Signature Option                        |
| 20   |        | SCPS Capabilities                           |
| 21   |        | Selective Negative Acknowledgements (SNACK) |
| 22   |        | Record Boundaries                           |
| 23   |        | Corruption Experienced                      |
| 24   |        | SNAP                                        |
| 25   |        | Unassigned (released 12/18/2000)            |
| 26   |        | TCP Compression Filter                      |

1. For more information on TCP options, refer to the *Security Guide, Cisco ACE Application Control Engine*.

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Maps table.
  - Click **Next** to accept your entries and to add another parameter map.
- 

**Related Topics**

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

# Configuring Optimization Parameter Maps

Use this procedure to configure an Optimization parameter map for use with a Layer 3/Layer 4 policy map.

See the “[Configuring Application Acceleration and Optimization](#)” section on page 13-1 or the *Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance* for more information about application acceleration and optimization.

## Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > Optimization Parameter Maps**. The Optimization Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The Optimization Parameter Maps configuration screen appears.
- Step 3** In the Parameter Name field, enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 4** Configure the Optimization parameter map using the information in [Table 8-5](#).

**Table 8-5 Optimization Parameter Map Attributes**

| Field                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                                | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.                                                                                                                                                                                                                                                                                                                                    |
| Set Browser Freshness Period               | Select the method that the ACE is to use to determine the freshness of objects in the client’s browser: <ul style="list-style-type: none"> <li>N/A—This option is not configured.</li> <li>Disable Browser Object Freshness Control—Browser freshness control is not to be used</li> <li>Set Freshness Similar To Flash Forward Objects—The ACE is to set freshness similar to that used for FlashForwarded objects and to use the values specified in the Maximum Time for Cache Time-To-Live and Minimum Time for Cache Time-To-Live fields.</li> </ul> |
| Duration For Browser Freshness (Seconds)   | This field appears if the Set Browser Freshness Period option is not configured.<br>Enter the number of seconds that objects in the client’s browser are considered fresh. Valid entries are 0 to 2147483647 seconds.                                                                                                                                                                                                                                                                                                                                     |
| Response Codes To Ignore (Comma Separated) | Enter a comma-separated list of HTTP response codes for which the response body must not be read. For example, an entry of 302 indicates that the ACE is to ignore the response body of a 302 (redirect) response from the origin server. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters and integers from 100 to 599, inclusive.                                                                                                                                                                                   |
| Appscope Optimize Rate (%)                 | Enter the percentage of all requests or sessions to be sampled for performance with acceleration (or optimization) applied. All applicable optimizations for the class will be performed. Valid entries are from 0 to 100 percent, with a default of 10 percent. The sum of this value and the value entered in the Passthru Rate Percent field must not exceed 100.                                                                                                                                                                                      |
| Appscope Passthrough Rate (%)              | Enter the percentage of all requests or sessions to be sampled for performance without optimization. No optimizations for the class will be performed. Valid entries are from 0 to 100, with a default of 10 percent. The sum of this value and the value entered in the Optimize Rate Percent field must not exceed 100.                                                                                                                                                                                                                                 |

Table 8-5 Optimization Parameter Map Attributes (continued)

| Field                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max. Number for Parameter Summary Log (Bytes)   | Enter the maximum number of bytes that are to be logged for each parameter value in the parameter summary of a transaction log entry in the statistics log. If a parameter value exceeds this limit, it is truncated at the specified limit. Valid entries are 0 to 10,000 bytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Max. For Post Data to Scan for Logging (KBytes) | Enter the maximum number of kilobytes of POST data the ACE is to scan for parameters for the purpose of logging transaction parameters in the statistics log.<br>Valid entries are 0 to 1000 KB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| String For Grouping Requests                    | Enter the string the ACE is to use to sort requests for AppScope reporting. The string can contain a URL regular expression that defines a set of URLs in which URLs that differ only by their query parameters are to be treated as separate URLs in AppScope reports.<br><br>For example, to define a string that is used to identify the URLs <code>http://server/catalog.asp?region=asia</code> and <code>http://server/catalog.asp?region=america</code> as two separate reporting categories, you would enter <code>http_query_param(region)</code> .<br><br>Valid entries contain 1 to 255 characters and can contain the parameter expander functions listed in Table 8-6.                                                                                                                                                                          |
| Base File Anonymous Level                       | Information that is common to a large set of users is generally not confidential or user-specific. Conversely, information that is unique to a specific user or a small set of users is generally confidential or user-specific. The anonymous base file feature enables the ACE to create and deliver condensed base files that contain only information that is common to a large set of users. No information unique to a particular user, or across a very small subset of users, is included in anonymous base files.<br><br>Enter the value for base file anonymity for the all-user condensation method. Valid entries are integers from 0 to 50; the default value of 0 disables the base file anonymity feature.                                                                                                                                   |
| Cache-Key Modifier Expression                   | A cache object key is a unique identifier that is used to identify a cached object to be served to a client, replacing a trip to the origin server. The cache key modifier feature allows you to modify the canonical form of a URL; that is, the portion before “?” in a URL. For example, the canonical URL of “ <code>http://www.xyz.com/somepage.asp?action=browse&amp;level=2</code> ” is “ <code>http://www.xyz.com/somepage.asp</code> ”.<br><br>Enter a regular expression containing embedded variables as described in Table 8-6. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here.<br><br>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. If the string includes spaces, enclose the string with quotation marks (“”). |
| Min. Time For Cache Time-To-Live (Seconds)      | Enter the minimum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. This value specifies the minimum time that content can be cached. If the ACE is configured for FlashForward optimization, this value should normally be 0. If the ACE is configured for dynamic caching, this value should indicate how long the ACE should cache the page. (See Table 5-16 for information about these configuration options.)<br><br>Valid entries are 0 to 2147483647 seconds.                                                                                                                                                                                                                                                                                                                       |
| Max. Time For Cache Time-To-Live (Seconds)      | Enter the maximum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. Valid entries are 0 to 2147483647 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 8-5 Optimization Parameter Map Attributes (continued)

| Field                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cache Time-To-Live Duration (%)                      | <p>Enter the percent of an object's age at which an embedded object without an explicit expiration time is considered fresh.</p> <p>Valid entries are 0 to 100 percent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Expression To Modify Cache Key Query Parameter       | <p>The cache parameter feature allows you to modify the query parameter of a URL; that is, the portion after “?” in a URL. For example, the query parameter portion of “http://www.xyz.com/somepage.asp?action=browse&amp;level=2” is “action=browse&amp;level=2”.</p> <p>Enter a regular expression containing embedded variables as described in Table 8-6. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. If no string is specified, the query parameter portion of the URL is used as the default value for this portion of the cache key.</p> <p>Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters.</p> |
| Canonical URL Expressions (Comma Separated)          | <p>The ACE uses the canonical URL feature to eliminate the “?” and any characters that follow to identify the general part of the URL. This general URL is then used to create the base file. In this way, the ACE maps multiple URLs to a single canonical URL.</p> <p>Enter a comma-separated list of parameter expander functions as defined in Table 8-6 to identify the URLs to associate with this parameter map.</p> <p>Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters.</p>                                                                                                                                                                                                              |
| Enable Cacheable Content Optimization                | <p>This feature allows the ACE to detect content that can be cached and perform delta optimization on it.</p> <p>Check the check box to enable delta optimization of content that can be cached. Clear the check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Enable Delta Optimization On First Visit To Web Page | <p>Check the check box to enable condensation on the first visit to a Web page. Clear the check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Min. Page Size For Delta Optimization (Bytes)        | <p>Enter the minimum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Max. Page Size For Delta Optimization (Bytes)        | <p>Enter the maximum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Set Default Client Script                            | <p>Indicate the scripting language that the ACE is to recognize on condensed content pages:</p> <ul style="list-style-type: none"> <li>• N/A—This option is not configured.</li> <li>• Javascript—The default scripting language is JavaScript.</li> <li>• Visual Basic Script—The default scripting language is Visual Basic.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                              |
| Exclude Iframes From Delta Optimization              | <p>Check the check box to indicate that delta optimization is not to be applied to IFrames (inline frames). Clear the check box to indicate that delta optimization is to be applied to IFrames.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Exclude Non-ASCII Data From Delta Optimization       | <p>Check the check box to indicate that delta optimization is not to be applied to non-ASCII data. Clear the check box to indicate that delta optimization is to be applied to non-ASCII data.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table 8-5 Optimization Parameter Map Attributes (continued)

| Field                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exclude JavaScripts From Delta Optimization   | Check the check box to indicate that delta optimization is not to be applied to JavaScript. Clear the check box to indicate that delta optimization is to be applied to JavaScript.                                                                                                                                                                                                                                                                                                                                                          |
| MIME Types To Exclude From Delta Optimization | <ol style="list-style-type: none"> <li>1. In the first field, enter a comma-separated list of the MIME (Multipurpose Internet Mail Extension) type messages that are not to have delta optimization applied, such as image/Jpeg, text/html, application/msword, or audio/mpeg. See <a href="#">Supported MIME Types, page 8-25</a> for a list of supported MIME types.</li> <li>2. Click <b>Add</b> to add the entry to the list box on the right. You can position the entries in the list box by using the Up and Down buttons.</li> </ol> |
| Remove HTML META Elements From Documents      | Check the check box to indicate that HTML META elements are to be removed from documents to prevent them from being condensed. Clear the check box to indicate that HTML META elements are not to be removed from documents.                                                                                                                                                                                                                                                                                                                 |
| Set Flash Forward Refresh Policy              | <p>Select the method the ACE is to use to refresh stale embedded objects:</p> <ul style="list-style-type: none"> <li>• N/A—This option is not configured.</li> <li>• Allow Flash Forward To Indirect Refresh Of Objects—The ACE is to use FlashForward to indirectly refresh embedded objects.</li> <li>• Bypass Flash Forward To Direct Refresh Of Objects—The ACE is to bypass FlashForward for stale embedded objects so that they are refreshed directly.</li> </ul>                                                                     |
| Rebase Delta Optimization Threshold (%)       | <p>Enter the delta threshold, expressed as a percent, when rebasing is to be triggered. This entry represents the size of a page delta relative to total page size, expressed as a percent. This entry triggers rebasing when the delta response size exceeds the threshold as a percentage of base file size.</p> <p>Valid entries are 0 to 10000 percent.</p>                                                                                                                                                                              |
| Rebase Flash Forward Threshold (%)            | <p>Enter the threshold, expressed as a percent, when rebasing is to be triggered based on the percent of FlashForwarded URLs in the response. This entry triggers rebasing when the difference between the percentages of FlashForwarded URLs in the delta response and the base file exceeds the threshold.</p> <p>Valid entries are 0 to 10000 percent.</p>                                                                                                                                                                                |
| Rebase History Size (Pages)                   | <p>Enter the number of pages to be stored before the ACE resets all rebase control parameters to zero and starts over. This option prevents the base file from becoming too rigid.</p> <p>Valid entries are 10 to 2147483647.</p>                                                                                                                                                                                                                                                                                                            |
| Rebase Modify Cool-Off Period (Seconds)       | <p>Enter the number of seconds after the last modification before performing a rebase.</p> <p>Valid entries are 1 to 14400 seconds (4 hours).</p>                                                                                                                                                                                                                                                                                                                                                                                            |
| Rebase Reset Period (Seconds)                 | <p>Enter the period of time, in seconds, for performing a meta data refresh.</p> <p>Valid entries are 1 to 900 seconds (15 minutes).</p>                                                                                                                                                                                                                                                                                                                                                                                                     |
| Override Client Request Headers               | <p>Indicate how the ACE is to handle client request headers (primarily for embedded objects):</p> <ul style="list-style-type: none"> <li>• N/A—This feature is not enabled.</li> <li>• All Cache Request Headers Are Ignored—The ACE is to ignore all cache request headers.</li> <li>• Overrides The Cache Control: No Cache HTTP Header From A Request—The ACE is to ignore cache control request headers that state <i>no cache</i>.</li> </ul>                                                                                           |



Table 8-5 Optimization Parameter Map Attributes (continued)

| Field                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Override Server Response Headers         | <p>Indicate how the ACE is to handle origin server response headers (primarily for embedded objects):</p> <ul style="list-style-type: none"> <li>• N/A—This feature is not enabled.</li> <li>• All Cache Request Headers Are Ignored—The ACE is to ignore all response headers.</li> <li>• Overrides The Cache Control: Private HTTP Header From A Response—The ACE is to ignore cache control response headers that state <i>private</i>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| UTF-8 Character Set Threshold            | <p>The UTF-8 (8-bit Unicode Transformation Format) character set is an international standard that allows Web pages to display non-ASCII or non-English multibyte characters. It can represent any universal character in the Unicode standard and is backwards compatible with ASCII.</p> <p>Enter the number of UTF-8 characters that need to appear on a page to constitute a UTF-8 character set page. Valid entries are integers from 1 to 1,000,000.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server Load Threshold Trigger (%)        | <p>The server load threshold trigger indicates that the time-to-live (TTL) period for cached objects is to be based dynamically on server load. With this method, TTL periods increase if the current response time from the origin sever is greater than the average response time and decrease if the current response time from the origin server is less than the average response time when the difference in response times exceeds a specified threshold amount.</p> <p>Enter the threshold, expressed as a percent, at which the TTL for cached objects is to be changed. Valid entries are from 0 to 100 percent.</p>                                                                                                                                                                                                                                                                                                                                                                            |
| Server Load Time-To-Live Change (%)      | <p>This option specifies the percentage by which the cache TTL is increased or decreased in response to a change in server load. For example, if this value is set to 20 and the current TTL for a response is 300 seconds, and if the current server response times exceeds the trigger threshold, the cache TTL for the response is raised to 360 seconds.</p> <p>Enter the percent by which the cache TTL is to be increased or decreased when the server load threshold trigger is met.</p> <p>Valid entries are from 0 to 100 percent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Delta Optimization Mode                  | <p>Select the method by which delta optimization is to be implemented:</p> <ul style="list-style-type: none"> <li>• N/A—This option is not configured.</li> <li>• Enable The All-User Mode For Delta Optimization—The ACE is to generate the delta against a single base file that is shared by all users of the URL. This option is usable in most cases if the structure of a page is common across all users, and the disk space overhead is minimal.</li> <li>• Enable The Per-User Mode For Delta Optimization—The ACE is to generate the delta against a base file that is created specifically for that user. This option is useful when page contents, including layout elements, are different for each user, and delivers the highest level of condensation. However, this increases disk space requirements because a copy of the base page that is delivered to each user is cached. This option is useful when privacy is required because base pages are not shared among users.</li> </ul> |
| String To Be Used For Server HTTP Header | <p>Use this option to define a string that is to be sent in the server header for an HTTP response. This option provides you with a method for uniquely tagging the context or URL match statement by setting the server header value to a particular string. The server header string can be used when a particular URL is not being transmitted to the correct target context or match statement.</p> <p>Enter the string that is to appear in the server header. Valid entries are quoted text strings with a maximum of 64 alphanumeric characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 8-6 lists the parameter expander functions that you can use.

**Table 8-6** *Parameter Expander Functions*

| Variable                                                                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>\$(number)</code>                                                                                                                   | <p>Expands to the corresponding matching subexpression (by <i>number</i>) in the URL pattern. Subexpressions are marked in a URL pattern using parentheses (). The numbering of the subexpressions begins with 1 and is the number of the left-parenthesis “(“ counting from the left. You can specify any positive integer for the number. <code>\$(0)</code> matches the entire URL. For example, if the URL pattern is <code>((http://server/.*)/(.*)/a.jsp)</code>, and the URL that matches it is <code>http://server/main/sub/a.jsp?category=shoes&amp;session=99999</code>, then the following are correct:</p> <p><code>\$(0)</code> = <code>http://server/main/sub/a.jsp</code><br/> <code>\$(1)</code> = <code>http://server/main/sub/</code><br/> <code>\$(2)</code> = <code>http://server/main</code><br/> <code>\$(3)</code> = <code>sub</code></p> <p>If the specified subexpression does not exist in the URL pattern, then the variable expands to the empty string.</p> |
| <code>\$http_query_string()</code>                                                                                                        | <p>Expands to the value of the whole query string in the URL. For example, if the URL is <code>http://myhost/dohis?param1=value1&amp;param2=value2</code>, then the following is correct:</p> <p><code>\$http_query_string()</code> = <code>param1=value1&amp;param2=value2</code></p> <p>This function applies to both GET and POST requests.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>\$http_query_param(query-param-name)</code><br><br>The obsolete syntax is also supported:<br><code>\$param(query-param-name)</code> | <p>Expands to the value of the named query parameter (case-sensitive). For example, if the URL is <code>http://server/main/sub/a.jsp?category=shoes&amp;session=99999</code>, then the following are correct:</p> <p><code>\$http_query_param(category)</code> = <code>shoes</code><br/> <code>\$http_query_param(session)</code> = <code>99999</code></p> <p>If the specified parameter does not exist in the query, then the variable expands to the empty string. This function applies to both GET and POST requests.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>\$http_cookie(cookie-name)</code>                                                                                                   | <p>Evaluates to the value of the named cookie. For example, <code>\$http_cookie(cookiexyz)</code>. The cookie name is case-sensitive.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>\$http_header(request-header-name)</code>                                                                                           | <p>Evaluates to the value of the specified HTTP request header. In the case of multivalued headers, it is the single representation as specified in the HTTP specification. For example, <code>\$http_header(user-agent)</code>. The HTTP header name is not case-sensitive.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <code>\$http_method()</code>                                                                                                              | <p>Evaluates to the HTTP method used for the request, such as GET or POST.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 8-6 Parameter Expander Functions (continued)

| Variable                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Boolean Functions:<br>\$http_query_param_present( <i>query-param-name</i> )<br>\$http_query_param_notpresent( <i>query-param-name</i> )<br>\$http_cookie_present( <i>cookie-name</i> )<br>\$http_cookie_notpresent( <i>cookie-name</i> )<br>\$http_header_present( <i>request-header-name</i> )<br>\$http_header_notpresent( <i>request-header-name</i> )<br>\$http_method_present( <i>method-name</i> )<br>\$http_method_notpresent( <i>method-name</i> ) | Evaluates to a Boolean value: True or False, depending on the presence or absence of the element in the request. The elements are a specific query parameter ( <i>query-param-name</i> ), a specific cookie ( <i>cookie-name</i> ), a specific request header ( <i>request-header-name</i> ), or a specific HTTP method ( <i>method-name</i> ). All identifiers are case-sensitive except for the HTTP request header name.                                                         |
| \$regex_match( <i>param1</i> , <i>param2</i> )                                                                                                                                                                                                                                                                                                                                                                                                             | Evaluates to a Boolean value: True if the two parameters match and False if they do not match. The two parameters can be any two expressions, including regular expressions, that evaluate to two strings. For example, this function:<br><pre>\$regex_match(\$http_query_param(URL), .*Store\.asp.*)</pre> compares the query URL with the regular expression string <code>.*Store\.asp.*</code> .<br>If the URL matches this regular expression, this function evaluates to True. |

**Step 5** Do the following:

- Click **Deploy Now** to save your entries. The ACE appliance validates the parameter map configuration and deploys it.
- Click **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Maps table.
- Click **Next** to accept your entries and to add another parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

## Configuring Generic Parameter Maps

Generic parameter maps allow you to specify nonprotocol-specific behavior for data parsing. Generic parameter maps examine the payload and make decisions regardless of the protocol.

Use this procedure to configure a generic parameter map.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > Generic Parameter Maps**. The Generic Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The Generic Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 8-7](#).

**Table 8-7**      *Generic Parameter Map Attributes*

| Field                     | Description                                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter Name            | Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                         |
| Description               | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs. |
| Case-Insensitive          | Check this check box to indicate that the ACE is to be case insensitive for this parameter map. Clear this check box to indicate that the ACE is to be case sensitive for this parameter map.                          |
| Max. Parse Length (Bytes) | Enter the number of bytes to parse for the total length of all generic headers. Valid entries are integers from 1 to 65535 with a default of 2048 bytes.                                                               |

- Step 4** Do the following:
- Click **Deploy Now** to deploy this configuration.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Generic Parameter Maps table.
  - Click **Next** to deploy your entries and to configure another generic parameter map.
- 

**Related Topics**

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

# Configuring RTSP Parameter Maps

RTSP parameter maps allow you to configure advanced RTSP behavior for server load-balancing connections.

Use this procedure to configure an [RTSP](#) parameter map.

## Procedure

- 
- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > RTSP Parameter Maps**. The RTSP Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The RTSP Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 8-8](#).

**Table 8-8** RTSP Parameter Map Attributes

| Field                            | Description                                                                                                                                                                                                            |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter Name                   | Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                         |
| Description                      | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs. |
| Case-Insensitive                 | Check this check box to indicate that the ACE is to be case insensitive. Clear this check box to indicate that the ACE is to be case sensitive.                                                                        |
| Header Max. Parse Length (Bytes) | Enter the number of bytes to parse for the total length of RTSP headers. Valid entries are integers from 1 to 65535 with a default of 2048 bytes.                                                                      |

- Step 4** Do the following:
- Click **Deploy Now** to deploy this configuration.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the RTSP Parameter Maps table.
  - Click **Next** to deploy your entries and to configure another RTSP parameter map.
- 

## Related Topics

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

# Configuring SIP Parameter Maps

SIP parameter maps allow you to configure SIP deep-packet inspection policy maps on the ACE.

Use this procedure to configure a SIP parameter map.

## Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > SIP Parameter Maps**. The SIP Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The SIP Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 8-9](#).

**Table 8-9** *SIP Parameter Map Attributes*

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter Name                    | Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                         |
| Description                       | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.                                                                                                                                                                                                                                                                                                 |
| Instant Messaging                 | Check the check box to enable instant messaging (IM) over SIP after it has been disabled. Clear this check box to disable this feature.                                                                                                                                                                                                                                                                                                                                                                                |
| Logging All                       | Check the check box to enable the logging of all received and transmitted packets in the system log (syslog). By default, the ACE disables the logging of these packets, however allows the logging of dropped SIP packets in the syslog.<br><br>The ACE allows all headers sent in the SIP packet, including proprietary headers. In the event of a failover for SIP sessions over UDP, the ACE continues to process SIP packets for established SIP sessions.<br><br>Clear this check box to disable this feature.   |
| Max. Forward Validation           | This option allows you to configure the ACE to validate the value of the Max-Forward header field.<br><br>Specify how the ACE is to handle the validation of Max-Forward header fields: <ul style="list-style-type: none"> <li>• N/A—The ACE is not to validate Max-Forward header fields.</li> <li>• Drop—The ACE is to drop the SIP message if it does not pass Max-Forward header validation.</li> <li>• Reset—The ACE is to reset the SIP connection if it does not pass Max-Forward header validation.</li> </ul> |
| Log Max. Forward Validation Event | Check the check box to indicate that the ACE is to log Max-Forward validation events. Clear the check box to disable this feature.                                                                                                                                                                                                                                                                                                                                                                                     |

Table 8-9 SIP Parameter Map Attributes (continued)

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mask UA Software Version            | <p>If the software version of a user agent is exposed, that user agent might be vulnerable to attacks from hackers who exploit the security holes present in that particular software version. This option allows you to mask or log the user agent software version so that it is not exposed.</p> <p>Check the check box to indicate that the ACE is to mask the user agent software version.</p> <p>Clear the check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Log UA Software Version             | <p>Check the check box to indicate that the ACE is to log the user agent software version.</p> <p>Clear the check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Strict Header Validation            | <p>You can ensure the validity of SIP packet headers by configuring the ACE to check for the presence of the following mandatory SIP header fields:</p> <ul style="list-style-type: none"> <li>• From</li> <li>• To</li> <li>• Call-ID</li> <li>• CSeq</li> <li>• Via</li> <li>• Max-Forwards</li> </ul> <p>If one of the header fields is missing in a SIP packet, the ACE considers that packet invalid. The ACE also checks for forbidden header fields, according to RFC 3261.</p> <p>Specify how the ACE is to handle header validation.</p> <ul style="list-style-type: none"> <li>• N/A—The ACE is not to perform header validation.</li> <li>• Drop—The ACE is to drop the SIP message if the SIP packet does not pass header validation.</li> <li>• Reset—The ACE is to reset the connection if the SIP packet does not pass header validation.</li> </ul> |
| Log Strict Header Validation        | <p>Check the check box to indicate that the ACE is to log header validation events.</p> <p>Clear the check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Mask Non SIP URI                    | <p>This option and the next enable the detection of non-SIP URIs in SIP messages.</p> <p>Check the check box to indicate that the ACE is to mask non-SIP URIs in SIP messages.</p> <p>Clear the check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Log Non SIP URI                     | <p>Check the check box to indicate that the ACE is to log non-SIP URIs in SIP messages.</p> <p>Clear the check box to disable this feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SIP Media Pinhole Timeout (Seconds) | <p>Specify the timeout period for SIP media pinhole (secure port) connections in seconds. Valid entries are integers from 1 to 65535 seconds. The default is 5 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration.
- Click **Cancel** to exit this procedure without saving your entries and to return to the SIP Parameter Maps table.
- Click **Next** to deploy your entries and to configure another SIP parameter map.

#### Related Topics

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

## Configuring Skinny Parameter Maps

Skinny Client Control Protocol ([SCCP](#) or [Skinny](#)) parameter maps allow you to configure SCCP packet inspection on the ACE.

Use this procedure to configure a Skinny parameter map.

#### Procedure

- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > Skinny Parameter Maps**. The Skinny Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The Skinny Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 8-10](#).

**Table 8-10** *Skinny Parameter Map Attributes*

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter Name       | Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                              |
| Description          | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.                                                                                                                                                                                                      |
| Enforce Registration | <p>You can configure the ACE to allow only registered Skinny clients to make calls. To accomplish this task, the ACE maintains the state of each Skinny client. After a client registers with <a href="#">CCM</a>, the ACE opens a secure port (pinhole) to allow that client to make a call.</p> <p>Check the check box to enable Skinny registration enforcement.</p> <p>Clear the check box to disable this feature.</p> |



Table 8-10 Skinny Parameter Map Attributes (continued)

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message Id Max.                 | <p>Enter the largest value for the station message ID in hexadecimal that the ACE is to accept. Valid entries are hexadecimal values from 0x0 to 0x4000. The default value is 0x181.</p> <p><b>Note</b> The Message Id Max. hexadecimal value should always start with 0x or 0X.</p> <p>If a packet arrives with a station message ID greater than the specified value, the ACE drops the packet and generates a syslog message.</p> |
| Min. SCCP Prefix Length (Bytes) | <p>By default, the ACE drops SCCP messages that have an SCCP Prefix length that is less than the message ID. The ACE drops Skinny message packets that fail this check and generates a syslog message.</p> <p>Enter the minimum SCCP prefix length in bytes. Valid entries are integers from 4 to 4000 bytes.</p>                                                                                                                    |
| Max. SCCP Prefix Length (Bytes) | <p>This feature allows you to configure the ACE so that it checks the maximum SCCP prefix length. The ACE drops Skinny message packets that fail this check and generates a syslog message.</p> <p>Enter the maximum SCCP prefix length in bytes. Valid entries are integers from 4 to 4000 bytes.</p>                                                                                                                               |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Skinny Parameter Maps table.
- Click **Next** to deploy your entries and to configure another Skinny parameter map.

#### Related Topics

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

## Configuring DNS Parameter Maps

Domain Name System (DNS) parameter maps allow you to configure DNS actions for DNS packet inspection.

Use this procedure to configure a DNS parameter map.

#### Procedure

- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > DNS Parameter Maps**. The DNS Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The DNS Parameter Maps configuration screen appears.

**Step 3** Configure the parameter map using the information in [Table 8-11](#).

**Table 8-11** *DNS Parameter Map Attributes*

| Field             | Description                                                                                                                                                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter Name    | Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                                                                                           |
| Description       | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.                                                                   |
| Timeout (Seconds) | Configure the ACE to time out DNS queries that have no matching server response. Specify the length of time in seconds that the ACE keeps the query entries without answers in the hash table before timing them out. Enter an integer from 2 to 120 seconds. The default is 10 seconds. |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration.
- Click **Cancel** to exit this procedure without saving your entries and to return to the DNS Parameter Maps table.
- Click **Next** to deploy your entries and to configure another DNS parameter map.

#### Related Topics

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

## Configuring RDP Parameter Maps

Remote Desktop Protocol (RDP) parameter maps configure routing-token-rebalance in which the ACE redirects connections that contain RDP packets to another server when the real server that matches the routing token information in the client request is down.

Use this procedure to configure a RDP parameter map.

#### Procedure

- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > RDP Parameter Maps**. The RDP Parameter Maps table appears.
- Step 2** From the RDP Parameter Maps table, click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The New Parameter Map configuration table appears.
- Step 3** From the New Parameter Map table, configure the parameter map using the information in [Table 8-11](#).

Table 8-12 RDP Parameter Map Attributes

| Field                   | Description                                                                                                                                                                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parameter Name          | Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                                          |
| Description             | Brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Double quotes must be entered as matching pairs.                  |
| Routing Token Rebalance | Check this check box to enable routing-token-rebalance.<br><br>Uncheck this check box to disable routing-token-rebalance and have the ACE drop the RDP packets when the real server that matches the routing token information is down. |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration.
- Click **Cancel** to exit this procedure without saving your entries and to return to the RDP Parameter Maps table.
- Click **Next** to deploy your entries and to configure another RDP parameter map.

**Related Topics**

- [Configuring Parameter Maps, page 8-1](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Contexts, page 4-1](#)

## Supported MIME Types

The ACE appliance supports following MIME types:

- application/msexcel
- application/mspowerpoint
- application/msword
- application/octet-stream
- application/pdf
- application/postscript
- application/^x-gzip
- application/^x-java-archive
- application/^x-java-vm
- application/^x-messenger
- application/^zip
- audio/\*
- audio/basic

- audio/midi
- audio/mpeg
- audio/x-adpcm
- audio/x-aiff
- audio/x-ogg
- audio/x-wav
- image/\*
- image/gif
- image/jpeg
- image/png
- image/tiff
- image/x-3ds
- image/x-bitmap
- image/x-niff
- image/x-portable-bitmap
- image/x-portable-greymap
- image/x-xpm
- text/\*
- text/css
- text/html
- text/plain
- text/richtext
- text/sgml
- text/xmcd
- text/xml
- video/\*
- video/flc
- video/mpeg
- video/quicktime
- video/sgi
- video/x-fli

## Viewing All Parameter Maps by Context

Use this procedure to view all parameter maps associated with a virtual context.

### Procedure

- 
- |               |                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select <b>Config &gt; Virtual Contexts</b> . The All Virtual Contexts table appears.                                                                                                                       |
| <b>Step 2</b> | Select the virtual context with the parameter maps you want to view, and then select <b>Load Balancing &gt; Parameter Maps</b> . The Parameter Maps table appears listing each parameter map and its type. |
- 

### Related Topics

- [Configuring Parameter Maps, page 8-1](#)





## CHAPTER 9

# Configuring SSL

---



### Note

The information in this chapter does not apply to the ACE NPE software version in which payload encryption protocols are removed (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

---

This chapter describes the steps required to configure your ACE appliance as a virtual Secure Sockets Layer (SSL) server for SSL initiation or termination.



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

The chapter contains the following section:

- [SSL Overview, page 9-2](#)
- [SSL Configuration Prerequisites, page 9-3](#)
- [Summary of SSL Configuration Steps, page 9-4](#)
- [SSL Setup Sequence, page 9-5](#)
- [Using SSL Certificates, page 9-6](#)
- [Using SSL Keys, page 9-11](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Generating CSRs, page 9-27](#)
- [Configuring SSL Proxy Service, page 9-28](#)
- [Configuring SSL OCSP Service, page 9-30](#)
- [Enabling Client Authentication, page 9-31](#)

## SSL Overview

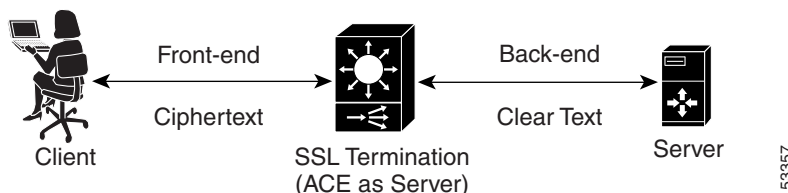
SSL is an application-level protocol that provides encryption technology for the Internet, ensuring secure transactions such as the transmission of credit card numbers for e-commerce Web sites. SSL initiation occurs when the ACE appliance acts as a client and initiates the SSL session between it and the SSL server. SSL termination occurs when the ACE, acting as an SSL server, terminates an SSL connection from a client and then establishes a TCP connection to an HTTP server.

SSL provides the secure transaction of data between a client and a server through a combination of privacy, authentication, and data integrity. SSL relies upon certificates and private-public key exchange pairs for this level of security.

Figure 9-1 shows the following network connections in which the ACE terminates the SSL connection with the client:

- Client to ACE—SSL connection between a client and the ACE acting as an SSL proxy server
- ACE to Server—TCP connection between the ACE and the HTTP server

**Figure 9-1** *SSL Termination with Client*



The ACE uses parameter maps, SSL proxy services, and class maps to build the policy maps that determine the flow of information between the client, the ACE, and the server. SSL termination is a Layer 3 and Layer 4 application because it is based on the destination IP addresses of the inbound traffic flow from the client. For this type of application, you create a Layer 3 and Layer 4 policy map that the ACE applies to the inbound traffic.

If you have a need to delete any of the SSL objects (auth groups, chain groups, parameter maps, keys, CRLs, or certificates), you must remove the dependency from within the proxy service first before removing the SSL object.

Before configuring the ACE for SSL, see [SSL Configuration Prerequisites, page 9-3](#).



# SSL Configuration Prerequisites

Before configuring your ACE for SSL operation, you must first ensure:

- Your ACE hardware is configured for server load balancing (SLB).



**Note** During the real server and server farm configuration process, when you associate a real server with a server farm, ensure that you assign an appropriate port number for the real server. The default behavior by the ACE is to automatically assign the same destination port that was used by the inbound connection to the outbound server connection if you do not specify a port.

- Your policy map is configured to define the SSL session parameters and client/server authentication tools, such as the certificate and RSA key pair.
- Your class map is associated with the policy map to define the virtual SSL server IP address that the destination IP address of the inbound traffic must match.
- You must import a digital certificate and its corresponding public and private key pair to the desired ACE context.
- At least one SSL certificate is available.
- If you do not have a certificate and corresponding key pair, you can generate an [RSA](#) key pair and a *certificate signing request (CSR)*. Create a CSR when you need to apply for a certificate from a *certificate authority (CA)*. The CA signs the CSR and returns the authorized digital certificate to you.

## RBAC User Role Requirements for SSL Configurations

For all SSL-related configurations on the ACE, a user with a custom role should include the following two rules as part of the assigned role:

- A rule that includes the SSL feature.
- A rule that includes the PKI feature.

For details on user roles and rules, see the [“Creating User Roles”](#) section in [Chapter 15, “Managing the ACE Appliance.”](#)

# Summary of SSL Configuration Steps

Table 9-1 describes the steps for using SSL keys and certificates.

**Table 9-1** *SSL Key and Certificate Procedure Overview*

|         | Task                                                                                                          | Description                                                                                                                                                                                                                                                                                                                              |
|---------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | Create an SSL parameter map.                                                                                  | Create an SSL parameter map to specify the options that apply to SSL sessions such as the method to be used to close SSL connections, the cipher suite, and version of SSL or TLS.<br><br>See <a href="#">Configuring SSL Parameter Maps, page 9-19</a> .                                                                                |
| Step 2  | Create an SSL key pair file.                                                                                  | Create an SSL RSA key pair file to generate a CSR, create a digital signature, and encrypt packet data during the SSL handshake with an SSL peer.<br><br>See <a href="#">Generating SSL Key Pairs, page 9-15</a> .                                                                                                                       |
| Step 3  | Configure CSR parameters.                                                                                     | Set CSR parameters to define the distinguished name attributes of a CSR.<br><br>See <a href="#">Configuring SSL CSR Parameters, page 9-26</a> .                                                                                                                                                                                          |
| Step 4  | Create a CSR.                                                                                                 | Create a CSR to submit with the key pair file when you apply for an SSL certificate.<br><br>See <a href="#">Generating CSRs, page 9-27</a> .                                                                                                                                                                                             |
| Step 5  | Copy and paste the CSR into the Certificate Authority (CA) Web-based application or e-mail the CSR to the CA. | Using the SSL key pair and CSR, apply for an approved certificate from a Certificate Authority.<br><br>Use the method specified by the CA for submitting your request.                                                                                                                                                                   |
| Step 6  | Save the approved certificate from the CA in its received format on an FTP, SFTP, or TFTP server.             | When you receive the approved certificate, save it in the format in which it was received on a network server accessible via FTP, SFTP, or TFTP.                                                                                                                                                                                         |
| Step 7  | Import the approved certificate and key pair into the desired virtual context.                                | Import the approved certificate and the associated SSL key pair into the appropriate context using ACE Appliance Device Manager.<br><br>See the following topics: <ul style="list-style-type: none"> <li>• <a href="#">Importing SSL Certificates, page 9-8</a></li> <li>• <a href="#">Importing SSL Key Pairs, page 9-12</a></li> </ul> |
| Step 8  | Confirm that the public key in the key pair file matches the public key in the certificate file.              | Examine the contents of the files to confirm that the key pair information is the same in both the key pair file and the certificate file.                                                                                                                                                                                               |
| Step 9  | Configure the virtual context for SSL.                                                                        | See <a href="#">Configuring Traffic Policies, page 12-1</a> .                                                                                                                                                                                                                                                                            |
| Step 10 | Configure auth group.                                                                                         | Create a group of certificates that are trusted as certificate signers by creating an authentication group. See <a href="#">Configuring SSL Authentication Groups, page 9-32</a> .                                                                                                                                                       |

Table 9-1 SSL Key and Certificate Procedure Overview (continued)

|         | Task                          | Description                                                                 |
|---------|-------------------------------|-----------------------------------------------------------------------------|
| Step 11 | Configure CRL.                | See <a href="#">Configuring CRLs for Client Authentication, page 9-33</a> . |
| Step 12 | Configure an SSL OCSP service | See <a href="#">Configuring SSL OCSP Service, page 9-30</a> .               |

For more information about using SSL with ACE appliances, see the *SSL Guide, Cisco ACE Application Control Engine*.

To configure ACE appliances for SSL, see the following topics:

- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL Proxy Service, page 9-28](#)
- [Configuring SSL OCSP Service, page 9-30](#)

## SSL Setup Sequence

The SSL setup sequence provides detailed instructions with illustrations for configuring SSL using the ACE Appliance Device Manager ([Figure 9-2](#)). The purpose of this option is to provide a visual guide for performing typical SSL operations, such as SSL CSR generation, SSL proxy creation, and so on. This option does not replace any existing SSL functions or configuration screens already present in ACE Appliance Device Manager. It is only intended as an additional guide for anyone unfamiliar or unclear with the SSL operations that need to be performed on the ACE. From the SSL setup sequence, you are allowed to configure all SSL operations, without duplicating the edit/delete/table/view operations that the other SSL configuration screens provide.

The purpose of this option is to provide details about typical SSL flows and the operations involved in performing typical SSL operations, including the following:

- SSL import/create keys
- SSL import certificates
- SSL CSR generation
- SSL proxy creation



### Note

The SSL Setup Sequence in the ACE Device Manager uses the terms *SSL Policies* and *SSL Proxy Service* interchangeably.

For more information on SSL configuration features, see [Summary of SSL Configuration Steps](#).

**Figure 9-2** *SSL Setup Sequence*



#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Using SSL Certificates

You can display a list of the certificates and their matching key pairs that are installed on the ACE for a context by choosing **Config > Virtual Contexts > context > Certificates**. The Certificates window appears, displaying the list of installed certificates.

Digital certificates and key pairs are a form of digital identification for user authentication. Certificate Authorities issue certificates that attest to the validity of the public keys they contain. A client or server certificate includes the following identification attributes:

- Name of the Certificate Authority and Certificate Authority digital signature
- Name of the client or server (the certificate subject) that the certificate authenticates
- Issuer
- Serial number
- Subject's matching public key of the certificate
- Time stamps that indicate the certificate's start date and expiration date
- CA certificate

A Certificate Authority has one or more signing certificates that it uses for creating SSL certificates and certificate revocation lists (CRL). Each signing certificate has a matching private key that is used to create the Certificate Authority signature. The Certificate Authority makes the signing certificates (with the public key embedded) available to the public, enabling anyone to access and use the signing certificates to verify that an SSL certificate or CRL was actually signed by a specific Certificate Authority.

**Note**


---

The ACE supports the creation of a maximum of eight CRLs for any context.

---

ACE appliances require certificates and corresponding key pairs for:

- **SSL termination**—The ACE appliance acts as an SSL proxy server and terminates the SSL session between it and the client. For SSL termination, you must obtain a server certificate and corresponding key pair.
- **SSL initiation**—The ACE appliance acts as a client and initiates the SSL session between it and the SSL server. For SSL initiation, you must obtain a client certificate and corresponding key pair.

The Matching Key column in the Certificates window (Config > Virtual Contexts > context > Certificates) displays the name of a key pair that ACE Appliance Device Manager was able to match up with certificate. If ACE Appliance Device Manager cannot detect a matching key pair for a certificate, it leaves the Matching Key table cell blank. If the number of unmatched certificates and key pairs exceeds 50, then ACE Appliance Device Manager leaves the entire Matching Key column blank, even when matching certificates and key pairs exist for the context. When this condition occurs, you can verify that a certificate and key pair match by using the SSL Setup Sequence feature.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > SSL > Setup Sequence**.  
The Setup Sequence window appears.
- Step 2** In the Setup Sequence window, click **Configure SSL Policies**.  
The Configure SSL Policies window appears.
- Step 3** From the Certificate drop-down list in the Configure SSL Policies - Basic Settings section, choose a certificate.
- Step 4** From the Keys drop-down list in the Configure SSL Policies - Basic Settings section, choose a key pair.
- Step 5** Click **Verify Key**.  
ACE Appliance Device Manager checks to see if the selected certificate and key pair match. A popup window appears to indicate if the two items match.
- 

**Note**


---

The ACE includes a preinstalled sample certificate and corresponding key pair. The certificate is for demonstration purposes only and does not have a valid domain. It is a self-signed certificate with basic extensions named *cisco-sample-cert*. The key pair is an RSA 1024-bit key pair named *cisco-sample-key*.

You can display the sample certificate and corresponding key pair files as follows:

- To display the *cisco-sample-cert* file, choose **Config > Virtual Contexts > context > SSL > Certificates**.
- To display the *cisco-sample-key* file, choose **Config > Virtual Contexts > context > SSL > Keys**.

You can add these files to an SSL-proxy service (see the [“Configuring SSL Proxy Service”](#) section on page 9-28) and are available for use in any context with the filenames remaining the same in each context.

The ACE allows you to export these files but does not allow you to import any files with these names. When you upgrade the ACE software, these files are overwritten with the files provided in the upgrade image. You cannot use the **crypto delete** CLI command to delete these files unless you downgrade the ACE software because a software downgrade preserves these files as if they were user-installed SSL files.

#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Exporting SSL Certificates, page 9-16](#)
- [Importing SSL Certificates, page 9-8](#)
- [Using SSL Keys, page 9-11](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Generating CSRs, page 9-27](#)

## Importing SSL Certificates

Use this procedure to import SSL certificates.



#### Note

The ACE supports a maximum of 4,096 certificates.

#### Assumptions

- You have configured an ACE appliance for server load balancing. (See [Load Balancing Overview, page 5-1](#).)
- You have obtained an SSL certificate from a certificate authority (CA) and have placed it on a network server accessible by the ACE appliance.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > SSL > Certificates**. The Certificates table appears, listing any valid SSL certificates.  
The cisco-sample-cert certificate is included in the list. For information on this sample certificate, see the [“Using SSL Certificates” section on page 9-6](#).
- Step 2** Click **Import**. The Import dialog box appears.  
To import multiple SSL certificates, click **Bulk Import**. The Bulk Import dialog box appears.



**Note** SSL bulk import can take longer based on the number of SSL certificates being imported. It will progress to completion on the ACE. To see the imported certificates in the ACE Device Manager, perform a CLI synchronization for this context once the SSL bulk import has completed. For information on synchronizing contexts, see the [“Synchronizing Virtual Context Configurations” section on page 4-79](#).

- Step 3** Enter the applicable information:
- For the Import dialog box, see [Table 9-2](#).
  - For the Bulk Import dialog box, see [Table 9-3](#).

**Table 9-2** *SSL Certificate Management Import Attributes*

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol         | Specify the method to be used for accessing the network server: <ul style="list-style-type: none"> <li>• FTP—Indicates that FTP is to be used to access the network server when importing the SSL certificate.</li> <li>• SFTP—Indicates that SFTP is to be used to access the network server when importing the SSL certificate.</li> <li>• TFTP—Indicates that TFTP is to be used to access the network server when importing the SSL certificate.</li> <li>• TERMINAL—Indicates that you will import the file using cut and paste by pasting the certificate information to the terminal display. You can only use the terminal method to display <a href="#">PEM</a> files, which are in ASCII format.</li> </ul> |
| IP Address       | This field appears for FTP, TFTP, and SFTP.<br>Enter the IPv4 address of the remote server on which the SSL certificate file resides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Remote File Name | This field appears for FTP, TFTP, and SFTP.<br>Enter the directory and filename of the certificate file on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Local File Name  | Enter the filename to be used for the SSL certificate file when it is imported to the ACE appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| User Name        | This field appears for FTP and SFTP.<br>Enter the name of the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Password         | This field appears for FTP and SFTP.<br>Enter the password for the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Confirm          | This field appears for FTP and SFTP.<br>Reenter the password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Passphrase       | This field appears for FTP, TFTP, SFTP, and TERMINAL.<br>Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted <a href="#">PEM</a> and <a href="#">PKCS</a> files.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 9-2** *SSL Certificate Management Import Attributes (continued)*

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                         |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confirm        | This field appears for FTP, SFTP, and TERMINAL.<br>Reenter the passphrase.                                                                                                                                                                                                                                                                                                          |
| Non-Exportable | The ability to export SSL certificates allows you to copy signed certificates to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting is similar to copying in that the original files are not deleted.<br><br>Check the check box to indicate that this certificate file cannot be exported from the ACE appliance. |
| Import Text    | This field appears for Terminal.<br><br>Cut the certificate information from the remote server and paste it into this field.                                                                                                                                                                                                                                                        |

**Table 9-3** *SSL Certificate Management Bulk Import Attributes*

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol       | SFTP is to be used to access the network server when importing the SSL certificates. SFTP is the only supported protocol for bulk import.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| IP Address     | Enter the IPv4 address of the remote server on which the SSL certificate files reside.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Remote Path    | Path to the SSL certificate files that reside on the remote server. The ACE fetches only files specified by the path; it does not recursively fetch remote directories. Enter a filename path including wildcards (for example, /remote/path/*.pem). The ACE supports POSIX pattern matching notation, as specified in section 2.13 of the “Shell and Utilities” volume of IEEE Std 1003.1-2004. This notation includes the “*,” “?” and “[ ” metacharacters.<br><br>To fetch all files from a remote directory, specify a remote path that ends with a wildcard character (for example, /remote/path/*). Do not include spaces or the following special characters:<br><br>; < > \   ' @ \$ & ()<br><br>The ACE fetches all files on the remote server that matches the wildcard criteria. However, it imports only files with names that have a maximum of 40 characters. If the name of a file exceeds 40 characters, the ACE does not import the file and discards it. |
| User Name      | Enter the name of the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Password       | Enter the password for the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Confirm        | Reenter the password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Passphrase     | Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Confirm        | Reenter the passphrase.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Non-Exportable | The ability to export SSL certificates allows you to copy signed certificates to another server on your network so that you can then import them onto another ACE or Web server. Exporting is similar to copying in that the original files are not deleted.<br><br>Check the check box to specify that this certificate file cannot be exported from the ACE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



**Step 4** Do the following:

- Click **OK** to accept your entries and to return to the Certificates table. The ACE Appliance Device Manager updates the Certificates table with the newly installed certificate.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Certificates table.
- 

#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Using SSL Keys, page 9-11](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Using SSL Keys

An ACE appliance and its peer use a public key cryptographic system named Rivest, Shamir, and Adelman Signatures (RSA) for authentication during the SSL handshake to establish an SSL session. The RSA system uses *key pairs* that consist of a public key and a corresponding private (secret) key. During the handshake, the RSA key pairs encrypt the session key that both devices will use to encrypt the data that follows the handshake.

Use this procedure to view options for working with SSL and SSL keys.

#### Procedure

---

**Step 1** Choose **Config > Virtual Contexts > context > SSL > Keys**. The Keys table appears.

**Step 2** Continue with one of the following options:

- Generate a key pair—See [Generating SSL Key Pairs, page 9-15](#).
  - Import a key pair—See [Importing SSL Key Pairs, page 9-12](#).
  - Export a key pair—See [Exporting SSL Key Pairs, page 9-18](#).
  - Generate a CSR—See [Generating CSRs, page 9-27](#).
- 

#### Related Topics

- [Generating SSL Key Pairs, page 9-15](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Generating SSL Key Pairs, page 9-15](#)
- [Exporting SSL Key Pairs, page 9-18](#)
- [Configuring SSL, page 9-1](#)

## Importing SSL Key Pairs

Use this procedure to import an SSL key pair file.

**Note**

The ACE supports a maximum of 4,096 key pairs.

**Assumptions**

- You have configured an ACE appliance for server load balancing. (See [Load Balancing Overview, page 5-1.](#))
- You have obtained an SSL key pair from a certificate authority (CA) and have placed the pair on a network server accessible by the ACE appliance.

**Procedure**

**Step 1** Choose **Config > Virtual Contexts > context > SSL > Keys**. The Keys table appears, listing existing SSL keys.

The cisco-sample-key key pair is included in the list. For information on this sample key pair, see the [“Using SSL Certificates” section on page 9-6.](#)

**Step 2** Click **Import**. The Import dialog box appears.

To import multiple SSL key pairs, click **Bulk Import**. The Bulk Import dialog box appears.

**Note**

SSL bulk import can take longer based on the number of SSL keys being imported. It will progress to completion on the ACE. To see the imported keys in the ACE Device Manager, perform a CLI synchronization for this *context* once the SSL bulk import has completed. For information on synchronizing contexts, see the [“Synchronizing Virtual Context Configurations” section on page 4-79.](#)

**Step 3** Enter the applicable information as follows:

- For the Import dialog box, see [Table 9-4.](#)
- For the Bulk Import dialog box, see [Table 9-5.](#)

**Table 9-4** *SSL Key Pair Import Attributes*

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol         | Specify the method to be used for accessing the network server: <ul style="list-style-type: none"> <li>FTP—Indicates that FTP is to be used to access the network server when importing the SSL key pair file.</li> <li>SFTP—Indicates that SFTP is to be used to access the network server when importing the SSL key pair file.</li> <li>TFTP—Indicates that TFTP is to be used to access the network server when importing the SSL key pair file.</li> <li>TERMINAL—Indicates that you will import the file using cut and paste by pasting the certificate and key pair information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.</li> </ul> |
| IP Address       | This field appears for FTP, TFTP, and SFTP.<br>Enter the IPv4 address of the remote server on which the SSL key pair file resides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Remote File Name | This field appears for FTP, TFTP, and SFTP.<br>Enter the directory and filename of the key pair file on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Local File Name  | Enter the filename to be used for the SSL key pair file when it is imported to the ACE appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| User Name        | This field appears for FTP and SFTP.<br>Enter the name of the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Password         | This field appears for FTP and SFTP.<br>Enter the password for the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Confirm          | This field appears for FTP and SFTP.<br>Reenter the password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Passphrase       | This field appears for FTP, TFTP, SFTP, and TERMINAL.<br>Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Confirm          | This field appears for FTP, SFTP, and TERMINAL.<br>Reenter the passphrase.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Non-Exportable   | The ability to export SSL key pair files allows you to copy key pair files to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting is similar to copying in that the original files are not deleted.<br><br>Check the check box to indicate that this key pair file cannot be exported from the ACE appliance. Clear the check box to indicate that this key pair file can be exported from the ACE appliance.                                                                                                                                                                                                                                    |
| Import Text      | This field appears for Terminal.<br>Cut the key pair information from the remote server and paste it into this field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table 9-5 *SSL Key Pair Bulk Import Attributes*

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol       | SFTP is to be used to access the network server when importing the SSL key pairs. SFTP is the only supported protocol for bulk import.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IP Address     | Enter the IPv4 address of the remote server on which the SSL key pair files resides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Remote Path    | <p>Enter the path to the key pair files that reside on the remote server. The ACE fetches only files specified by the path; it does not recursively fetch remote directories. Enter a filename path including wildcards (for example, /remote/path/*.pem). The ACE supports POSIX pattern matching notation, as specified in section 2.13 of the “Shell and Utilities” volume of IEEE Std 1003.1-2004. This notation includes the “*”, “?” and “[” metacharacters.</p> <p>To fetch all files from a remote directory, specify a remote path that ends with a wildcard character (for example, /remote/path/*). Do not include spaces or the following special characters:</p> <p style="text-align: center;">; &lt; &gt; \   ' @ \$ &amp; ( )</p> <p>The ACE fetches all files on the remote server that matches the wildcard criteria. However, it imports only files with names that have a maximum of 40 characters. If the name of a file exceeds 40 characters, the ACE does not import the file and discards it.</p> |
| User Name      | Enter the name of the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Password       | Enter the password for the user account on the network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Confirm        | Reenter the password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Passphrase     | Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Confirm        | Reenter the passphrase.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Non-Exportable | Check this check box to specify that this certificate file cannot be exported from the ACE. The ability to export SSL key pairs allows you to copy signed certificates to another server on your network so that you can then import them onto another ACE or Web server. Exporting is similar to copying in that the original files are not deleted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Step 4** Do the following:

- Click **OK** to accept your entries and to return to the Keys table. The ACE Appliance Device Manager updates the Keys table with the imported key pair file information.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Keys table.

**Related Topics**


- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Configuring SSL Parameter Maps, page 9-19](#)

- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Generating SSL Key Pairs

If you do not have any matching key pairs, you can use the ACE appliance to generate a key pair. Use this procedure to generate SSL RSA key pairs.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > SSL > Keys**. The Keys table appears.
- Step 2** Click **Add** to add a new key pair. The Keys configuration screen appears.
- 

**Note** You cannot modify an existing entry in the Keys table. Instead, delete the existing entry, and then add a new one.
- 
- Step 3** In the Name field, enter the name of the SSL key pair. Valid entries are alphanumeric strings with a maximum of 40 characters.
- Step 4** In the Size field, select the key pair security strength. The number of bits in the key pair file defines the size of the RSA key pair used to secure Web transactions. Longer keys produce more secure implementations by increasing the strength of the RSA security policy. Options and their relative levels of security are as follows:
- 512—Least security
  - 768—Normal security
  - 1024—High security, level 1
  - 1536—High security, level 2
  - 2048—High security, level 3
  - 4096—High security, level 4
- Step 5** In the Type field, specify **RSA** as the public-key cryptographic system used for authentication.
- Step 6** In the Exportable Key field, check the check box to indicate that the key pair file can be exported. Clear the check box to indicate that the key pair file cannot be exported.
- Step 7** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Keys table.
  - Click **Next** to save your entries and to define another RSA key pair.
-

After generating an RSA key pair, you can:

- Create a CSR parameter set. The CSR parameter set defines the distinguished name attributes for the ACE appliance to use during the CSR-generating process. For details on defining a CSR parameter set, see the [Configuring SSL CSR Parameters, page 9-26](#).
- Generate a CSR for the RSA key pair file and transfer the CSR request to the certificate authority for signing. This provides an added layer of security because the RSA private key originates directly within the ACE appliance and does not have to be transported externally. Each generated key pair must be accompanied by a corresponding certificate to work. For details on generating a CSR, see [Generating CSRs, page 9-27](#).

#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Exporting SSL Certificates

The ability to export SSL certificates allows you copy signed certificates to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting certificates is similar to copying in that the original certificates are not deleted.

Use this procedure to export SSL certificates from an ACE appliance to a remote server.

#### Assumption

- The SSL certificate can be exported. (See [Importing SSL Certificates, page 9-8](#).)
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

#### Procedure

- 
- |               |                                                                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; SSL &gt; Certificates</b> . The Certificates table appears, listing any valid SSL certificates. |
| <b>Step 2</b> | Select the certificate you want to export, and then click <b>Export</b> . The Export dialog box appears.                                                 |
| <b>Step 3</b> | Enter the information in <a href="#">Table 9-6</a> .                                                                                                     |

Table 9-6 *SSL Certificate Export Attributes*

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol         | Specify the method to be used for exporting the SSL certificate: <ul style="list-style-type: none"> <li>FTP—Indicates that FTP is to be used to access the network server when exporting the SSL certificate.</li> <li>SFTP—Indicates that SFTP is to be used to access the network server when exporting the SSL certificate.</li> <li>TFTP—Indicates that TFTP is to be used to access the network server when exporting the SSL certificate.</li> <li>TERMINAL—Indicates that you will export the certificate using cut and paste by pasting the certificate and key pair information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.</li> </ul> |
| IP Address       | This field appears for FTP, TFTP, and SFTP.<br>Enter the IPv4 address of the remote server to which the SSL certificate file is to be exported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Remote File Name | This field appears for FTP, TFTP, and SFTP.<br>Enter the directory and filename to be used for the SSL certificate file on the remote network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| User Name        | This field appears for FTP and SFTP.<br>Enter the name of the user account on the remote network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Password         | This field appears for FTP and SFTP.<br>Enter the password for the user account on the remote network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Confirm          | This field appears for FTP and SFTP.<br>Reenter the password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Step 4** Do the following:

- Click **OK** to export the certificate and to return to the Certificates table.
- Click **Cancel** to exit this procedure without exporting the certificate and to return to the Certificates table.

**Related Topics**

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Generating SSL Key Pairs, page 9-15](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Exporting SSL Key Pairs

The ability to export SSL key pairs allows you copy SSL key pair files to another server on your network so that you can then import them onto another ACE appliance or Web server. Exporting key pair files is similar to copying in that the original key pairs are not deleted.

Use this procedure to export SSL key pairs from an ACE appliance to a remote server.

### Assumption

The SSL key pair can be exported (see [Generating SSL Key Pairs, page 9-15](#)).

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > SSL > Keys**. The Keys table appears.
- Step 2** Select the key entry you want to export, and then click **Export**. The Export dialog box appears.
- Step 3** Enter the information in [Table 9-7](#).

**Table 9-7** *SSL Key Export Attributes*

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol         | Specify the method to be used for exporting the SSL key pair: <ul style="list-style-type: none"> <li>FTP—Indicates that FTP is to be used to access the network server when exporting the SSL key pair.</li> <li>SFTP—Indicates that SFTP is to be used to access the network server when exporting the SSL key pair.</li> <li>TFTP—Indicates that TFTP is to be used to access the network server when exporting the SSL key pair.</li> <li>TERMINAL—Indicates that you will export the key pair using cut and paste by pasting the key pair information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.</li> </ul> |
| IP Address       | This field appears for FTP, TFTP, and SFTP.<br>Enter the IPv4 address of the remote server to which the SSL key pair is to be exported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Remote File Name | This field appears for FTP, TFTP, and SFTP.<br>Enter the directory and filename to be used for the SSL key pair file on the remote network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| User Name        | This field appears for FTP and SFTP.<br>Enter the name of the user account on the remote network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Password         | This field appears for FTP and SFTP.<br>Enter the password for the user account on the remote network server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Confirm          | This field appears for FTP and SFTP.<br>Reenter the password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



**Step 4** Do the following:

- Click **OK** to export the key pair and to return to the Keys table.
- Click **Cancel** to exit this procedure without exporting the key pair and to return to the Keys table.

#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Generating SSL Key Pairs, page 9-15](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Configuring SSL Parameter Maps

An SSL parameter map defines the SSL session parameters that an ACE appliance applies to an SSL proxy service. SSL parameter maps let you apply the same SSL session parameters to different proxy services.

Use this procedure to create SSL parameter maps.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > SSL > Parameter Maps**. The Parameter Maps table appears.
- Step 2** Click **Add** to add a new SSL parameter map, or select an existing entry to modify, and then click **Edit**. The Parameter Map configuration screen appears.
- Step 3** In the Parameter Map Name field, enter a unique name for the parameter map. Valid entries are alphanumeric strings with a maximum of 64 characters.
- Step 4** In the Description field, enter a brief description of the parameter map. Enter a text string with a maximum of 240 alphanumeric characters (A–Z, a–z, 0–9). Spaces and special characters are allowed. Enter double quotes as matching pairs.
- Step 5** In the Queue Delay Timeout (Milliseconds) field, set the amount of time (in milliseconds) to wait before emptying the queued data for encryption. The default delay is 200 milliseconds, and can be adjusted from 0 (disabled) to 10000. If disabled (set to 0), the ACE encrypts the data from the server as soon as it arrives and then sends the encrypted data to the client.



**Note** The Queue Delay Timeout is only applied to data that the SSL module sends to the client. This avoids a potentially long delay in passing a small HTTP GET to the real server.

- Step 6** In the Session Cache Timeout (Milliseconds) field, specify a timeout value of an SSL session ID to remain valid before the ACE requires the full SSL handshake to establish a new SSL session. This value allows the ACE to reuse the master key on subsequent connections with the client, which can speed up

the SSL negotiation process. The default value is 300 seconds (5 minutes), and can be adjusted from 0 (to indicate an infinite timeout, so that session IDs are removed from the cache only when the cache becomes full), up to 72000 seconds (20 hours). Specifying 0 causes the ACE to implement a least recently used (LRU) timeout policy. By disabling this option, the full SSL handshake occurs for each new connection with the ACE.

**Step 7** In the Reject Expired CRLs field, click the check box to specify whether expired CRLs can be used. If checked, no expired CRLs are allowed.

**Step 8** In the Close Protocol Behavior field, select the method to be used to close the SSL connection:

- **Disabled**—Indicates that the ACE appliance is to send a close-notify alert message to the SSL peer; however, the SSL peer does not expect a close-notify alert before removing the session. Whether the SSL peer sends a close-notify alert message or not, the session information is preserved, allowing session resumption for future SSL connections.
- **None**—Indicates that the ACE appliance is not to send a close-notify alert message to the SSL peer, nor does the ACE appliance expect a close-notify alert message from the peer. The ACE appliance preserves the session information so that SSL resumption can be used for future SSL connections.

**Step 9** In the SSL Version field, enter the version of SSL to be used during SSL communications:

- **All**—Indicates that the ACE appliance is to use both SSL v3 and TLS v1 in its communications with peer ACE appliances.
- **SSL3**—Indicates that the ACE appliance is to use only SSL v3 in its communications with peer ACE appliances.
- **TLS1**—Indicates that the ACE appliance is to use only TLS v1 in its communications with peer ACE appliances.
- **TLS1\_1**—Indicates that the ACE appliance is to use only TLS Version 1.1 in its communication with peer ACE appliances.
- **TLS1\_2**—Indicates that the ACE appliance is to use only TLS Version 1.2 in its communication with peer ACE appliances.
- **Upto\_TLS1\_1**—Indicates all SSL versions upto TLS 1.1.
- **Upto\_TLS1\_2**—Indicates all SSL versions upto TLS 1.2.



**Note** For TLS1\_1 and TLS1\_2 SSL versions, only certain ‘Ciphers’ are supported as mentioned in the tables below. If the user tries to configure any unsupported SSL version or unsupported Cipher, an error message will be displayed.

Following tables show the list of supported cipher suites for TLS1\_1 and TLS1\_2 in ACE”

**Table 9-8** Cipher suites supported by TLS 1.1

| Cipher Suite Name         | Cipher Suite Number |
|---------------------------|---------------------|
| RSA_WITH_RC4_128_MD5      | { 0x00,0x04 }       |
| RSA_WITH_RC4_128_SHA      | { 0x00,0x05 }       |
| RSA_WITH_DES_CBC_SHA      | { 0x00,0x09 }       |
| RSA_WITH_3DES_EDE_CBC_SHA | { 0x00,0x0A }       |
| RSA_WITH_AES_128_CBC_SHA  | { 0x00,0x2F }       |
| RSA_WITH_AES_256_CBC_SHA  | { 0x00,0x35 }       |

Table 9-9

Table 9-10 Cipher suites supported by TLS 1.2

| Cipher Suite Name           | Cipher Suite Number |
|-----------------------------|---------------------|
| RSA_WITH_RC4_128_MD5        | { 0x00,0x04 }       |
| RSA_WITH_RC4_128_SHA        | { 0x00,0x05 }       |
| RSA_WITH_3DES_EDE_CBC_SHA   | { 0x00,0x0A }       |
| RSA_WITH_AES_128_CBC_SHA    | { 0x00,0x2F }       |
| RSA_WITH_AES_256_CBC_SHA    | { 0x00,0x35 }       |
| RSA_WITH_AES_128_CBC_SHA256 | { 0x00,0x3C }       |

**Step 10** In the Ignore Authentication Failure field, check the check box to ignore expired or invalid client or server certificates and to continue setting up the SSL connection. Clear the check box to return to the default setting of disabled. This field allows the ACE appliance to ignore the following nonfatal errors with respect to either client certificates for SSL termination configurations, or server certificates for SSL initiation configurations:

- Certificate not yet valid (both)
- Certificate has expired (both)
- Certificate revoked (both)
- Unknown issuer (both)
- No client certificate (client certificate only)
- CRL not available (client certificate only)
- CRL has expired (client certificate only)
- Certificate has signature failure (client certificate only)
- Certificate other error (client certificate only)

**Step 11** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The updated Parameter Map screen appears along with the Parameter Map Cipher table. Continue with [Step 12](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Parameter Map table.
- Click **Next** to save your entries and to define another parameter map.

- Step 12** In the Parameter Map Cipher table, click **Add** to add a cipher, or select an existing cipher, and then click **Edit**. The Parameter Map Cipher configuration screen appears.
- Enter the information in [Table 9-11](#).

**Table 9-11** *SSL Parameter Map Cipher Configuration Attributes*

| Field           | Description                                                                                                                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cipher Name     | Cipher to use.<br><br>For more information on the SSL cipher suites that ACE supports, see <i>SSL Guide, Cisco ACE Application Control Engine</i> .                                                                                                                                                                                      |
| Cipher Priority | Priority that you want to assign to this cipher suite. The priority indicates the cipher's preference for use.<br><br>Valid entries are from 1 to 10 with 1 indicating the least preferred and 10 indicating the most preferred. When determining which cipher suite to use, the ACE chooses the cipher suite with the highest priority. |

- Step 13** In the Parameter Map Cipher table, do one of the following:
- **Deploy Now** to deploy this configuration on the ACE appliance.
  - **Cancel** to exit the procedure without saving your entries and to return to the Parameter Map Cipher table.
  - **Next** to save your entries and to add another entry to the Parameter Map Cipher table.
- Step 14** Click the **Redirect Authentication Failure** tab and click **Add** to add a redirect or choose an existing redirect, and click **Edit**.
- Enter the information in [Table 9-12](#).



**Note**

The Redirect Authentication Failure feature is only for SSL termination configurations in which the ACE performs client authentication. The ACE ignores these attributes if you configure them for an SSL initiation configuration.

**Table 9-12** *SSL Parameter Map Redirect Configuration Attributes*

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client Certificate Validation | <p>Select the type of certificate validation failure to redirect. From the drop-down list, choose the type to redirect:</p> <ul style="list-style-type: none"> <li>Any—Associates any of the certificate failures with the redirect. You can configure the authentication-failure redirect any command with individual reasons for redirection. When you do, the ACE attempts to match one of the individual reasons before using the any reason. You cannot configure the authentication-failure redirect any command with the authentication-failure ignore command.</li> <li>Cert-expired—Associates an expired certificate failure with a redirect.</li> <li>Cert-has-signature-failure—Associates a certificate signature failure with a redirect.</li> <li>Cert-not-yet-valid—Associates a certificate that is not yet valid failure with the redirect.</li> <li>Cert-other-error—Associates a all other certificate failures with a redirect.</li> <li>Cert-revoked—Associates a revoked certificate failure with a redirect.</li> <li>CRL-has-expired—Associates an expired CRL failure with a redirect.</li> <li>CRL-not-available—Associates a CRL that is not available failure with a redirect.</li> <li>No-client-cert—Associates no client certificate failure with a redirect.</li> <li>Unknown-issuer—Associates an unknown issuer certificate failure with a redirect.</li> </ul> |
| Redirect Type                 | <p>Select the redirect type to use:</p> <ul style="list-style-type: none"> <li>Server Farm—Specifies a server farm for the redirect.</li> <li>URL—Specifies a static URL path for the redirect.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Server Farm Name              | <p>This field appears when the <a href="#">Redirect Type</a> is set to Server Farm. The ACE Device Manager displays all configured host and redirect server farms. Choose one of the available server farm options or click <b>Plus (+)</b> to open the server farm configuration popup and configure a redirect server farm (see the <a href="#">“Configuring Server Farms”</a> section on page 6-18).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Redirect URL                  | <p>This field appears when the Redirect Type is set to URL. Enter the static URL path for the redirect. Enter a string with a maximum of 255 characters and no spaces.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Redirect Code                 | <p>This field appears when the Redirect Type is set to URL.</p> <p>Enter the redirect code that is sent back to the client:</p> <ul style="list-style-type: none"> <li>301—Status code for a resource permanently moving to a new location.</li> <li>302—Status code for a resource temporarily moving to a new location.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Step 15** In the Redirect Authentication Failure table, do one of the following:

- Click **Deploy Now** to deploy the Redirect Authentication Failure table on the ACE and save your entries to the running-configuration and startup-configuration files.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Redirect Authentication Failure table.
- Click **Next** to deploy your entries and to add another entry to the Redirect Authentication Failure table.

**Step 16** In the Parameter Map table, do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Parameter Map table.
  - Click **Next** to deploy your entries and to add another entry to the Parameter Map table.
- 

#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Generating SSL Key Pairs, page 9-15](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Proxy Service, page 9-28](#)

# Configuring SSL Chain Group Parameters


A chain group specifies the *certificate chains* that the ACE appliance sends to its peer during the handshake process. A certificate chain is a hierarchal list of certificates that includes the ACE appliance's certificate, the root certificate authority certificate, and any intermediate certificate authority certificates. Using the information provided in a certificate chain, the certificate verifier searches for a trusted authority in the certificate hierarchal list up to and including the root certificate authority. If the verifier finds a trusted authority before reaching the root certificate authority certificate, it stops searching further.

Use this procedure to configure certificate chains for a virtual context.

## Assumption

At least one SSL certificate is available.

## Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > SSL > Chain Group Parameters**. The Chain Group Parameters table appears.
- Step 2** Click **Add** to add a new chain group, or select an existing chain group, and then click **Edit** to modify it. The Chain Group Parameters configuration screen appears.
- Step 3** In the Name field, enter a unique name for the chain group. Valid entries are alphanumeric strings with a maximum of 64 characters.
- Step 4** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance. The updated Chain Group Parameters screen appears along with the Chain Group Certificates table. Continue with [Step 5](#).
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Chain Group Parameters table.
  - Click **Next** to save your entries and to add another entry to the Chain Group Parameters table.
- Step 5** In the Chain Group Certificates table, click **Add** to add an entry. The Chain Group Certificates configuration screen appears.
- 

**Note** You cannot modify an existing entry in the Chain Group Certificates table. Instead, delete the entry, and then add a new one.
- 
- Step 6** In the Certificate Name field, select the certificate to add to this chain group.
- Step 7** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Chain Group Certificates table.
  - Click **Next** to save your entries and to add another certificate to this chain group table.
-

**Related Topics**

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Generating SSL Key Pairs, page 9-15](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Configuring SSL CSR Parameters

A *certificate signing request* (CSR) is a message you send to a certificate authority such as VeriSign and Thawte to apply for a digital identity certificate. The CSR contains information that identifies the SSL site, such as location and a serial number, and a public key that you choose. A corresponding private key is not included in the CSR, but is used to digitally sign the request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for more information.

If the request is successful, the certificate authority returns a digitally signed (with the private key of the certificate authority) identity certificate.

CSR parameters define the *distinguished name* attributes the ACE appliance applies to the CSR during the CSR-generating process. These attributes provide the certificate authority with the information it needs to authenticate your site. Defining a CSR parameter set lets you to generate multiple CSRs with the same distinguished name attributes.

Each context on an ACE appliance can contain up to eight CSR parameter sets.

Use this procedure to define the distinguished name attributes for SSL CSRs.

**Procedure**

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; SSL &gt; CSR Parameters</b> . The CSR Parameters table appears.                                                                                                                                                                                                                                                   |
| <b>Step 2</b> | Click <b>Add</b> to add new set of CSR attributes, or select an existing entry to modify, and then click <b>Edit</b> . The CSR Parameters configuration screen appears.                                                                                                                                                                                                    |
| <b>Step 3</b> | In the Name field, enter a unique name for this parameter set. Valid entries are alphanumeric strings with a maximum of 64 characters.                                                                                                                                                                                                                                     |
| <b>Step 4</b> | In the Country field, enter the name of the country where the SSL site resides. Valid entries are 2 alphabetic characters representing the country, such as <i>US</i> for the United States. The International Organization for Standardization (ISO) maintains the complete list of valid country codes on its Web site ( <a href="http://www.iso.org">www.iso.org</a> ). |
| <b>Step 5</b> | In the State field, enter the name of the state or province where the SSL site resides.                                                                                                                                                                                                                                                                                    |
| <b>Step 6</b> | In the Locality field, enter the name of the city where the SSL site resides.                                                                                                                                                                                                                                                                                              |
| <b>Step 7</b> | In the Common Name field, enter the name of the domain or host of the SSL site. Valid entries are alphanumeric strings with a maximum of 64 characters. The ACE supports the following special characters: , . / = + - ^ @ ! % ~ # \$ * ( ).                                                                                                                               |



- Step 8** In the Serial Number field, enter a serial number to assign to the certificate. Valid entries are alphanumeric strings with a maximum of 16 characters.
- Step 9** In the Organization Name field, enter the name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.
- Step 10** In the Email field, enter the site e-mail address. Valid entries are alphanumeric strings with a maximum of 40 characters.
- Step 11** In the Organization Unit field, enter the name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.
- Step 12** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the CSR Parameters table.
  - Click **Next** to save your entries and to define another set of CSR attributes.
- 

#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Generating CSRs

A *certificate signing request* (CSR) is a message you send to a certificate authority such as VeriSign and Thawte to apply for a digital identity certificate. Create a CSR when you need to apply for a certificate from a certificate authority. When the certificate authority approves a request, it signs the CSR and returns the authorized digital certificate to you. This certificate includes the private key of the certificate authority. When you receive the authorized certificate and key pair, you can import them for use (see [Importing SSL Certificates, page 9-8](#) and [Importing SSL Key Pairs, page 9-12](#)).

Use this procedure to generate SSL CSRs.

#### Assumption

- You have configured SSL CSR parameters (see [Configuring SSL CSR Parameters, page 9-26](#)).
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

#### Procedure

---

- Step 1** Choose **Config > Virtual Contexts > context > SSL > Keys**. The Keys table appears.
- Step 2** Select a key in the table, and then click **Generate CSR**. The Generate a Certificate Signing Request dialog box appears.

**Step 3** In the CSR Parameter field, select the CSR parameter to be used.

**Step 4** Do the following:

- Click **OK** to generate the CSR. The CSR appears in a popup window which you can now submit to a certificate authority for approval. Work with your certificate authority to determine the method of submission, such as e-mail or a Web-based application. Click **Close** to close the popup window and to return to the Keys table.
- Click **Cancel** to exit this procedure without generating the CSR and to return to the Keys table.

#### Related Topics

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Configuring SSL Proxy Service

SSL proxy service defines the SSL parameter map, key pair, certificate, and chain group an ACE appliance uses during SSL handshakes. By configuring an SSL proxy *server* service on an ACE appliance, the ACE appliance can act as an SSL server.

Use this procedure to define the attributes that the ACE appliance is to use during SSL handshakes so that it can act as an SSL server.

#### Assumption

You have configured at least one SSL key pair, certificate, chain group, or parameter map to apply to this proxy service.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > SSL > Proxy Service**. The Proxy Service table appears.
- Step 2** Click **Add** to add a new proxy service, or select an existing service, and then click **Edit** to modify it. The Proxy Service configuration screen appears.
- Step 3** In the Name field, enter a unique name for this proxy service. Valid entries are alphanumeric strings with a maximum of 64 characters.
- Step 4** In the Keys field, select the key pair that the ACE appliance is to use during the SSL handshake for data encryption.



#### Caution

When choosing the key pair from the drop-down list, be sure to choose the keys that correspond to the certificate that you choose.

**Note**

If you use SSL Setup Sequence to create the proxy service, ACE appliance Device Manager selects the keys that correspond to the certificate that you choose. If ACE appliance Device Manager cannot detect a corresponding key pair, you can select a key pair from the drop-down list and click **Verify Key** to have ACE appliance Device Manager verify that the keys correspond to the selected certificate. ACE appliance Device Manager displays a message to let you know that your key pair selection either matches or does not match the selected certificate. For more information about SSL Setup Sequence, see the “[SSL Setup Sequence](#)” section on page 9-5.

The **cisco-sample-key** option is available for the sample key pair. For information about this sample key pair, see the “[Using SSL Certificates](#)” section on page 9-6.

- Step 5** In the Certificates field, select the certificate that the ACE appliance is to use during the SSL handshake to prove its identity.

**Caution**

When choosing the certificate from the drop-down list, be sure to choose the certificate that corresponds to the keys that you choose.

**Note**

If you use SSL Setup Sequence to create the proxy service, ACE appliance Device Manager selects the keys that correspond to the certificate that you choose. If ACE appliance Device Manager cannot detect a corresponding key pair, you can select a key pair from the drop-down list and click **Verify Key** to have ACE appliance Device Manager verify that the keys correspond to the selected certificate. ACE appliance Device Manager displays a message to let you know that your key pair selection either matches or does not match the selected certificate. For more information about SSL Setup Sequence, see the “[SSL Setup Sequence](#)” section on page 9-5.

The **cisco-sample-cert** option is available for the sample certificate. For information on this sample certificate, see the “[Using SSL Certificates](#)” section on page 9-6.

- Step 6** In the Chain Groups field, select the chain group that the ACE appliance is to use during the SSL handshake.
- Step 7** For the Auth Groups field, perform either of the following:
- Select N/A when authentication is not applicable for this proxy service. Then, proceed to [Step 11](#).
  - Select the auth group name that the ACE is to use during the SSL handshake. To create an auth group, see [Configuring SSL Authentication Groups](#), page 9-32.
- Step 8** Check the CRL Best-Effort check box to allow the ACE appliance to search client certificates for the service to determine if it contains a CRL in the extension. The ACE appliance then retrieves the value, if it exists.
- Clear the check box to display the CRL name field to select the CRL name.
- Step 9** For the CRL Name field, perform either of the following:
- Select N/A when the CRL name is not applicable.
  - Select the CRL name that the ACE used for authentication.
- Step 10** Check the OCSP Best-Effort check box to allow the ACE appliance to extract the extension to find the OCSP server information from the certificate itself where, from the revocation status, information about the certificate could be obtained. If this extension is missing from the certificate and the best effort OCSP server information is configured with the SSL proxy, the cert is considered revoked.
- Clear the check box to display the OCSP server field to select the available OCSP server.

- Step 11** In the Parameter Maps field, select the SSL parameter map to associate with this SSL proxy server service.
- Step 12** For the Revcheck priority order, select one of the following to set the priority for the revocation check:
- N/A—Indicates that this field is not applicable.
  - CRL-OCSP—The ACE uses the CRLs first to determine the revocation status, and then the OCSP servers.
  - OCSP-CRL—The ACE uses the OCSP servers first to determine the revocation status, and then the CRLs.
- Step 13** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Proxy Service table.
  - Click **Next** to save your entries and to add another proxy service.
- 

**Related Topics**

- [Configuring SSL, page 9-1](#)
- [Importing SSL Certificates, page 9-8](#)
- [Importing SSL Key Pairs, page 9-12](#)
- [Configuring SSL Parameter Maps, page 9-19](#)
- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring SSL CSR Parameters, page 9-26](#)
- [Configuring SSL OCSP Service, page 9-30](#)

## Configuring SSL OCSP Service

SSL Online Certificate Status Protocol (OCSP) service defines the host server for certificate revocation checks using OCSP. The OCSP server, also known as the OCSP responder, maintains or obtains the information about the certificates issued by different CAs that are revoked and possibly non-revoked, and provides this information when requested by OCSP clients. OCSP can provide latest information about the revocation status of the certificate. Use of OCSP removes the need to download and cache the CRLs which could be very large in sizes and impose large memory requirements on systems.

You can configure a maximum of 64 OCSP server configurations system-wide on the ACE. You can configure all of these servers in a single or multiple contexts.

Use this procedure to define the attributes that the ACE appliance is to use during SSL handshakes so that it can act as an SSL server.

**Assumption**

Configure OCSP on an associated proxy service.

You can configure both OCSP and CRLs for authentication.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > SSL > OCSP Service**. The OCSP Service table appears.
- Step 2** Click **Add** to add a new OCSP service, or select an existing service, and then click **Edit** to modify it. The OCSP Service configuration screen appears.
- Step 3** In the Name field, enter a unique name for this OCSP service. Valid entries are alphanumeric strings with a maximum of 64 characters. This name is used when you apply this configuration to an SSL proxy service.
- Step 4** In the URL field, enter an HTTP based URL for the OCSP host name and optional port ID in the form of `http://ocsp_hostname.com:port_id`. If you do not specify a port ID, the ACE uses the default value of 2560.
- Step 5** Optionally, in the Request Signer's Certificate field, you can select a file name for the signer certificate to sign the requests to the server. By default, the request is not signed.
- Step 6** Optionally, in the Response Signer's Certificate field, you can select a file name for the signer certificate to verify the signature on the server responses. By default, the responses are not verified.
- Step 7** Check the Enable Nonce check box to enable the inclusion of the nonce in the requests to the server. By default, nonce is disabled (unchecked).  
Clear the check box to disable the inclusion of the nonce in requests to the server.
- Step 8** In the TCP Connection Inactivity Timeout field, enter an integer from 2 to 3600 to specify the TCP connection inactivity timeout in seconds. The default is 300 seconds.
- Step 9** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the OCSP Service table.
  - Click **Next** to save your entries and to add another proxy service.
- 

### Related Topics

- [Configuring SSL, page 9-1](#)
- [Configuring SSL Proxy Service, page 9-28](#)

## Enabling Client Authentication

During the flow of a normal SSL handshake, the SSL server sends its certificate to the client. Then the client verifies the identity of the server through the certificate. However, the client does not send any identification of its own to the server. When you enable the client authentication feature enabled on the ACE, it will require that the client send a certificate to the server. Then the server verifies the following information on the certificate:

- A recognized CA issued the certificate.
- The valid period of the certificate is still in effect.
- The certificate signature is valid and not tampered.
- The CA has not revoked the certificate.

- At least one SSL certificate is available.

Use the following procedures to enable or disable client authentication:

- [Configuring SSL Proxy Service, page 9-28](#)
- [Configuring SSL Authentication Groups, page 9-32](#)
- [Configuring CRLs for Client Authentication, page 9-33](#)

## Configuring SSL Authentication Groups

On the ACE, you can implement a group of certificates that are trusted as certificate signers by creating an authentication group. After creating the authentication group and assigning its certificates, then you can assign the authentication group to a proxy service in an SSL termination configuration to enable client authentication. For information on client authentication, see [Enabling Client Authentication, page 9-31](#).


For information on server authentication and assigning an authentication group, see [Configuring SSL Proxy Service, page 9-28](#).

Use this procedure to specify the certificate authentication groups that the ACE uses during the SSL handshake and enable client authentication on this SSL-proxy service. The ACE includes the certificates configured in the group along with the certificate that you specified for the SSL proxy service.

### Assumptions

- At least one SSL certificate is available.
- Your ACE appliance supports authentication groups.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > SSL > Auth Group Parameters**.
- The Auth Group Parameters table appears.
- Step 2** Click **Add** to add a authentication group, or select an existing auth group, and then click **Edit** to modify it. The Auth Group Parameters configuration screen appears.
- Step 3** In the Name field, enter a unique name for the auth group. Valid entries are alphanumeric strings with a maximum of 64 characters.
- Step 4** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE. The updated Auth Group Parameters screen appears along with the Auth Group Certificates table. Continue with [Step 5](#).
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Auth Group Parameters table.
  - Click **Next** to deploy your entries and to add another entry to the Auth Group Parameters table.
- Step 5** In the Auth Group Certificate field, click **Add** to add an entry. The Auth Group Certificates configuration screen appears.
-  **Note** You cannot modify an existing entry in the Auth Group Certificates table. Instead, delete the entry, and then add a new one.
- 
- Step 6** In the Certificate Name field, select the certificate to add to this auth group.

- Step 7** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Auth Group Parameters table.
  - Click **Next** to deploy your entries and to add another entry to the Auth Group Parameters table.
- Step 8** You can repeat the previous step to add more certificates to the auth group or click **Deploy Now**.
- Step 9** After you configure auth group parameters, you can configure the SSL proxy service to use a CRL. See [Configuring CRLs for Client Authentication, page 9-33](#).

**Note**

When you enable client authentication, a significant performance decrease may occur. Additional latency may occur when you configure CRL retrieval.

**Related Topics**

- [Configuring SSL Chain Group Parameters, page 9-25](#)
- [Configuring CRLs for Client Authentication, page 9-33](#)

## Configuring CRLs for Client Authentication

By default, ACE does not use certificate revocation lists (CRLs) during client authentication. You can configure the SSL proxy service to use a CRL by having the ACE scan each client certificate for the service to determine if it contains a CRL in the extension and then retrieve the value, if it exists. For more information about SSL termination on the ACE, see the *SSL Guide, Cisco ACE Application Control Engine*.

**Note**

The ACE supports the creation of a maximum of eight CRLs for any context.

**Note**

When you enable client authentication, a significant performance decrease may occur. Additional latency may occur when you configure CRL retrieval.

Use this procedure to configure ACE to scan for CRLs and retrieve them.

**Assumption**

A CRL cannot be configured on an SSL proxy without first configuring an auth group.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > context > SSL > Certificate Revocation Lists (CRL)**. The Certificate Revocation List table appears.
- Step 2** Click **Add** to add a CRL or select an existing CRL, and then click **Edit** to modify it. The Certificate Revocation List screen appears.

**Step 3** Enter the information in [Table 9-13](#).

**Table 9-13** *SSL Certificate Revocation List*

| Field | Description                                                                                                                                                                                                                   |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name  | Enter the CRL name. Valid entries are unquoted alphanumeric strings with a maximum of 64 characters.                                                                                                                          |
| URL   | Enter the URL where the ACE retrieves the CRL. Valid entries are unquoted alphanumeric strings with a maximum of 255 characters. Only HTTP URLs are supported. ACE checks the URL and displays an error if it does not match. |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE. The updated Certificate Revocation List table appears.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Certificate Revocation List table.
- Click **Next** to deploy your entries and to add another entry to the Certificate Revocation List table.

#### Related Topics

- [Configuring SSL Proxy Service, page 9-28](#)
- [Configuring SSL Authentication Groups, page 9-32](#)





# CHAPTER 10

## Configuring Network Access

---

This chapter describes how to configure network access. The ACE appliance has four physical Ethernet interface ports. All VLANs are allocated to the physical ports. After the VLANs are assigned, you can configure the corresponding VLAN interfaces as either routed or bridged for use. When you configure an IP address on an interface, the ACE appliance automatically makes it a routed mode interface.

Similarly, when you configure a bridge group on an interface VLAN, the ACE appliance automatically makes it a bridged interface. Then, you associate a bridge-group virtual interface (BVI) with the bridge group.

The ACE appliance also supports shared VLANs; multiple interfaces in different contexts on the same VLAN within the same subnet. Only routed interfaces can share VLANs. Note that there is no routing across contexts even when shared VLANs are configured.

In routed mode, the ACE is considered a router hop in the network. In the Admin or user contexts, the ACE supports static routes only. The ACE supports up to eight equal cost routes for load balancing.



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

This chapter contains the following sections:

- [Configuring Port Channel Interfaces, page 10-2](#)
- [Configuring Gigabit Ethernet Interfaces, page 10-5](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context BVI Interfaces, page 10-23](#)
- [Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32](#)
- [Configuring Virtual Context Static Routes, page 10-34](#)
- [Configuring Global IP DHCP, page 10-35](#)

# Configuring Port Channel Interfaces

This section discusses how to configure port channel interfaces for the ACE appliance. It consists of the following topics:

- [Why Use Port Channels?, page 10-2](#)
- [Configuring a Port-Channel Interface, page 10-3](#)

## Why Use Port Channels?

A port channel groups multiple physical ports into a single logical port. This is also called “port aggregation” or “channel aggregation.” A port channel containing multiple physical ports has several advantages:

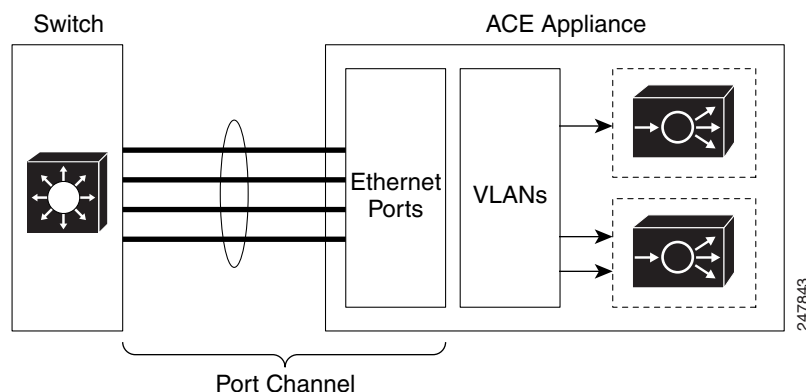
- Improves link reliability through physical redundancy.
- Allows greater total throughput to the ACE appliance. For example, four 1-Gigabit Ethernet interfaces can be aggregated into a single 4 Gigabit channel.
- Allows traffic capacity to be scaled up in the future, without network disruption at that time. A port channel can do everything a switched port can do, but a switched port cannot do everything a port channel can do. We recommend that you use a port channel.)
- Provides maximum flexibility of network configuration and focuses network configuration on VLANs rather than physical cabling

The disadvantage of a port channel is that it requires additional configuration on the switch the ACE is connected to, as well as the ACE itself. There are many methods of port aggregation implemented by different switches, and not every method works with ACE.

Using a port channel also requires more detailed knowledge of your network's VLANs, because all “cabling” to and from the ACE will be handled over VLANs rather than using physical cables. Nonetheless, use of port channels is highly recommended, especially in a production deployment of ACE.

[Figure 10-1](#) illustrates a port channel interface.

**Figure 10-1** Example of a Port Channel Interface



### Related Topic

[Configuring a Port-Channel Interface, page 10-3](#)

## Configuring a Port-Channel Interface

You can group physical ports together on the ACE to form a logical Layer 2 interface called the port-channel. All the ports belonging to the same port-channel must be configured with same values; for example, port parameters, VLAN membership, and trunk configuration. Only one port-channel in a channel group is allowed, and a physical port can belong to only to a single port-channel interface.

**Step 1** Choose **Config > Virtual Contexts > context > Network > Port Channel Interfaces**. The Port Channel Interfaces table appears.

**Step 2** Click **Add** to add a port channel interface, or select an existing port channel interface, and then click **Edit** to modify it.



**Note** If you click **Edit**, not all of the fields can be modified.

**Step 3** Enter the port channel interface attributes (see [Table 10-1](#)).

**Table 10-1** Port Channel Interface Attributes

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface Number      | Specify a channel number for the port-channel interface, which can be from 1 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description           | Enter a brief description for this interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Fault Tolerance VLAN  | Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Admin Status          | Indicate whether you want the interface to be Up or Down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Load Balancing Method | Specify one of the following load balancing methods: <ul style="list-style-type: none"> <li>• Dst-IP—Loads distribution on the destination IP address.</li> <li>• Dst-MAC—Loads distribution on the destination MAC address.</li> <li>• Dst-Port—Loads distribution on the destination TCP or UDP port.</li> <li>• Src-Dst-IP—Loads distribution on the source or destination IP address.</li> <li>• Src-Dst-MAC—Loads distribution on the source or destination MAC address.</li> <li>• Src-Dst-Port—Loads distribution on the source or destination port.</li> <li>• Src-IP—Loads distribution on the source IP address.</li> <li>• Src-MAC—Loads distribution on the source MAC address.</li> <li>• Src-Port—Loads distribution on the TCP or UDP source port.</li> </ul> |

Table 10-1 Port Channel Interface Attributes (continued)

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch Port Type | <p>Specify the interface switchport type:</p> <ul style="list-style-type: none"><li>• N/A—Indicates that the switchport type is not specified.</li><li>• Access—Specifies that the port interface is an access port. You must specify a VLAN as an access port in the Access VLAN field.</li><li>• Trunk—Specifies that the port interface is a trunk port. When you select Trunk, you must complete one of the following fields:<ul style="list-style-type: none"><li>– Trunk Native VLAN—Identifies the 802.1Q native VLAN for a trunk.</li><li>– Trunk Allowed VLANs—Selectively allocate individual VLANs to a trunk link.</li></ul></li></ul> |

**Step 4** Do the following:

- Click **Deploy Now** to save your entries and to return to the Port Channel Interface table.
- Click **Cancel** to exit the procedure without saving your changes and to return to the Port Channel Interface table.
- Click **Next** to save your entries and to add another port-channel interface.

**Step 5** (Optional) To display statistics and status information for a particular port-channel interface, choose the interface from the Port Channel Interfaces table, and click **Details**.

The **show interface port-channel** CLI command output appears. See the [“Displaying Port Channel Interface Statistics and Status Information”](#) section on page 10-5 for details.

## Displaying Port Channel Interface Statistics and Status Information

You can display statistics and status information for a particular port-channel interface.

### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; Network &gt; Port Channel Interfaces</b> .<br>The Port Channel Interfaces table appears.                                                                                                                                                                                               |
| <b>Step 2</b> | In the Port Channel Interfaces table, choose a port-channel interface from the Port Channel Interfaces table, and click <b>Details</b> .<br>The <b>show interface port-channel</b> CLI command output appears. For details about the displayed output fields, see the <i>Routing and Bridging Guide, Cisco ACE Application Control Engine</i> . |
| <b>Step 3</b> | (Optional) Click <b>Update Details</b> to refresh the display.                                                                                                                                                                                                                                                                                  |
| <b>Step 4</b> | Click <b>Close</b> to return to the Port Channel Interfaces table.                                                                                                                                                                                                                                                                              |
- 

### Related Topics

[Configuring a Port-Channel Interface, page 10-3](#)

## Configuring Gigabit Ethernet Interfaces

The ACE appliance provides physical Ethernet ports to connect servers, PCs, routers, and other devices to the ACE. The ACE supports four Layer 2 Ethernet ports for performing Layer 2 switching. You can configure the four Ethernet ports to provide an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks. Each Layer 2 Ethernet port supports autonegotiate, full-duplex, or half-duplex operation on an Ethernet LAN, and can carry traffic within a designated VLAN.

A Layer 2 Ethernet port can be configured as follows:

- **Member of Port-Channel Group**—The port is configured as a member of a port-channel group, which associates a physical port on the ACE to a logical port to create a port-channel logical interface. The VLAN association is derived from port-channel configuration. The port is configured as a Layer 2 EtherChannel, where each EtherChannel bundles the individual physical Ethernet data ports into a single logical link that provides the aggregate bandwidth of up to four physical links on the ACE.
- **Access VLAN**—The port is assigned to a single VLAN. This port is referred to as an access port and provides a connection for end users or node devices, such as a router or server.
- **Trunk port**—The port is associated with IEEE 802.1Q encapsulation-based VLAN trunking to allocate VLANs to ports and to pass VLAN information (including VLAN identification) between switches for all Ethernet channels defined in a Layer 2 Ethernet data port or a Layer 2 EtherChannel (port-channel) group on the ACE.

The following procedure describes how to configure a Gigabit Ethernet interface.

### Procedure

- 
- |               |                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; Network &gt; Gigabit Ethernet Interfaces</b> . The GigabitEthernet Interfaces table appears. |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|

- Step 2** Select an existing Gigabit Ethernet interface, and then click **Edit** to modify it.
- Step 3** Enter the Gigabit Ethernet physical interface attributes (see [Table 10-2](#)).

**Table 10-2** *Gigabit Ethernet Physical Interface Attributes*

| Field          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface Name | Name of the Gigabit interface, which is the <i>slot_number/port_number</i> where <i>slot_number</i> is the physical slot on the ACE for the specified port, and <i>port_number</i> is the physical Ethernet data port on the ACE for the specified port.                                                                                                                                                                                                                                                                                                                       |
| Description    | Enter a brief description for this interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Admin Status   | Indicate whether you want the interface to be Up or Down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Speed          | Specifies the port speed, which can be <ul style="list-style-type: none"> <li>• Auto—Autonegotiate with other devices</li> <li>• 10 Mbps</li> <li>• 100 Mbps</li> <li>• 1000 Mbps</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                   |
| Duplex         | Specifies an interface duplex mode, which can be: <ul style="list-style-type: none"> <li>• Auto—Resets the specified Ethernet port to automatically negotiate port speed and duplex of incoming signals. This is the default setting.</li> <li>• Half—Configures the specified Ethernet port for half-duplex operation. A half-duplex setting ensures that data only travels in one direction at any given time.</li> <li>• Full—Configures the specified Ethernet port for full-duplex operation, which allows data to travel in both directions at the same time.</li> </ul> |

**Table 10-2**      *Gigabit Ethernet Physical Interface Attributes (continued)*

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Operation Mode | <p>Specifies the port operation mode, which can be:</p> <ul style="list-style-type: none"> <li>• N/A—Indicates that this option is not to be used.</li> <li>• Channel Group—Specifies to map the port to a port channel. You must specify <ul style="list-style-type: none"> <li>– Port Channel Group Number—Specify the port channel group number</li> <li>– Fault Tolerant VLAN—Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group.</li> </ul> </li> <li>• Switch Port—Specifies the interface switchport type: <ul style="list-style-type: none"> <li>– Access —Specifies that the port interface is an access port. You must specify a VLAN as an access port in the Access VLAN field.</li> <li>– Trunk—Specifies that the port interface is a trunk port. When you select Trunk, you must complete only one of the following fields: <ul style="list-style-type: none"> <li>Trunk Native VLAN—Identifies the 802.1Q native VLAN for a trunk.</li> <li>Trunk Allowed VLANs—Selectively allocate individual VLANs to a trunk link.</li> </ul> </li> </ul> </li> </ul> |
| Fault Tolerant VLAN | Specifies the fault tolerant (FT) VLAN used for communication between the members of the FT group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table 10-2 Gigabit Ethernet Physical Interface Attributes (continued)

| Field         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Carrier Delay | <p>Adds a configurable delay at the physical port level to address any issues with transition time, based on the variety of peers. Valid values are 0 to 120 seconds. The default is 0 (no carrier delay).</p> <p><b>Note</b> If you connect an ACE to a Catalyst 6500 series switch, your configuration on the Catalyst may include the Spanning-Tree Protocol (STP). However, the ACE does not support STP. In this case, you may find that the Layer 2 convergence time is much longer than the physical port up time. For example, the physical port would normally be up within 3 seconds, but STP moving to the forward state may need approximately 30 seconds. During this transitional time, although the ACE declares the port to be up, the traffic will not pass. In this case, specify a carrier delay.</p>                                                                                  |
| QoS Trust COS | <p>Enables Quality of Service (QoS) for the physical Ethernet port. By default, QoS is disabled for each physical Ethernet port on the ACE.</p> <p>QoS for a configured physical Ethernet port based on VLAN Classes of Service (CoS) bits (priority bits that segment the traffic in eight different classes of service). When you enable QoS on a port (a trusted port), traffic is mapped into different ingress queues based on their VLAN CoS bits. If there are no VLAN CoS bits, or QoS is not enabled on the port (untrusted port), the traffic is then mapped into the lowest priority queue.</p> <p>You can enable QoS for an Ethernet port configured for fault tolerance. In this case, heartbeat packets are always tagged with COS bits set to 7 (a weight of High).</p> <p><b>Note</b> We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic.</p> |

**Step 4** Do the following:

- Click **Deploy Now** to save your entries and to return to the Physical Interface table.
- Click **Cancel** to exit the procedure without saving your changes and to return to the Physical Interface table.
- Click **Next** or **Previous** to go to the next or previous physical channel.
- Click **Delete** to remove this entry from the Physical Interface table and to return to the table.

**Step 5** (Optional) To display statistics and status information for a particular Gigabit Ethernet interface, choose the interface from the GigabitEthernet Interfaces table, and click **Details**.

The **show interface gigabitEthernet** CLI command output appears. See the [“Displaying Gigabit Ethernet Interface Statistics and Status Information”](#) section on page 10-9 for details.

**Related Topics**

- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context BVI Interfaces, page 10-23](#)
- [Configuring Virtual Context Static Routes, page 10-34](#)



## Displaying Gigabit Ethernet Interface Statistics and Status Information

You can display statistics and status information for a particular Gigabit Ethernet interface.

### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; Network &gt; GigabitEthernet Interfaces</b> .<br>The GigabitEthernet Interfaces table appears.                                                                                                                                                                                                   |
| <b>Step 2</b> | In the GigabitEthernet Interfaces table, choose a Gigabit Ethernet interface from the GigabitEthernet Interfaces table, and click <b>Details</b> .<br>The <b>show interface gigabitEthernet</b> CLI command output appears. For details on the displayed output fields, see the <i>Routing and Bridging Guide, Cisco ACE Application Control Engine</i> . |
| <b>Step 3</b> | (Optional) Click <b>Update Details</b> to refresh the display.                                                                                                                                                                                                                                                                                            |
| <b>Step 4</b> | Click <b>Close</b> to return to the GigabitEthernet Interfaces table.                                                                                                                                                                                                                                                                                     |
- 

### Related Topic

- [Configuring Gigabit Ethernet Interfaces, page 10-5](#)

# Configuring Virtual Context VLAN Interfaces

The ACE Appliance Device Manager uses class maps and policy maps to classify (filter) traffic and to direct it to different contexts. A virtual context uses VLANs to receive packets classified for that context.



## Note

When you create a new VLAN interface for a virtual context, you can configure one or more VLAN interfaces in any user context before you assign those VLAN interfaces to the associated user contexts in a virtual context through the Allocate-Interface VLANs field (see the [“Creating Virtual Contexts” section on page 4-2](#)).

Use this procedure to configure VLAN interfaces for virtual contexts.

## Procedure

- Step 1** To configure a virtual context, select **Config > Virtual Contexts > context > Network > VLAN Interfaces**. The VLAN Interface table appears.
- Step 2** Click **Add** to add a new VLAN interface, or select an existing VLAN interface, and then click **Edit** to modify it.



## Note

If you click **Edit**, not all of the fields can be modified.

- Step 3** Enter the VLAN interface attributes (see [Table 10-3](#)). Click **More Settings** to access the additional VLAN interface attributes. By default, ACE appliance Device Manager hides the default VLAN interface attributes and the VLAN interface attributes which are not commonly used.



## Note

If you create a fault-tolerant VLAN, do not use it for any other network traffic.

**Table 10-3** *VLAN Interface Attributes*

| Field       | Description                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------|
| VLAN        | Either accept the automatically incremented entry or enter a different value. Valid entries are integers from 2 to 4094. |
| Description | Enter a brief description for this interface.                                                                            |

Table 10-3 VLAN Interface Attributes (continued)


| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface Type    | <p>Select the role of the virtual context in the network topology of the VLAN interface:</p> <ul style="list-style-type: none"> <li>• <b>Routed</b>—In a routed topology, the ACE virtual context acts as a router between the client-side network and the server-side network. In this topology, every real server for the application must be routed through the ACE virtual context, either by setting the default gateway on each real server to the virtual contexts server-side VLAN interface address, or by using a separate router with appropriate routes configured between the ACE virtual context and the real servers.</li> </ul> <p> <b>Note</b> A routed VLAN interface can support both IPv4 and IPv6 addresses at the same time.</p> <ul style="list-style-type: none"> <li>• <b>Bridged</b>—In a bridged topology, the ACE virtual context bridges two VLANs, a client-side VLAN and a real-server VLAN, on the same subnet using a bridged virtual interface (BVI). In this case, the real server routing does not change to accommodate the ACE virtual context. Instead, the ACE virtual context becomes a “bump in the wire” that transparently handles traffic to and from the real servers.</li> <li>• <b>Unknown</b>—Choose Unknown if you are unsure of the network topology of the VLAN interface.</li> </ul> |
| IP Address        | <p>Enter the IPv4 address assigned to this interface. This address must be a unique IP address that is not used in another context. Duplicate IP addresses in different contexts are not supported.</p> <p>If this interface is only used for IPv6 traffic, entering an IPv4 address is optional.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Alias IP Address  | Enter the IPv4 address of the alias this interface is associated with.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Peer IP Address   | Enter the IPv4 address of the remote peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Netmask           | Select the subnet mask to be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Admin Status      | Indicate whether you want the interface to be Up or Down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Enable MAC Sticky | <p>Check the check box to indicate that the ACE appliance is to convert dynamic MAC addresses to sticky secure MAC addresses and add this information to the running configuration.</p> <p>Clear the check box to indicate that the ACE appliance is not to convert dynamic MAC addresses to sticky secure MAC addresses.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 10-3 VLAN Interface Attributes (continued)


| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Normalization | <p>Check the check boxes to indicate that normalization is to be enabled on this interface for IPv4, IPv6, or both.</p> <p>Clear the check box to indicate that normalization is to be disabled on this interface.</p> <div>  <p><b>Caution</b> Disabling normalization may expose your ACE appliance and network to potential security risks. Normalization protects your networking environment from attackers by enforcing strict security policies that are designed to examine traffic for malformed or malicious segments.</p> </div>                                                         |
| Enable IPv6          | <p>Check the check box to enable IPv6 on this interface. By default, IPv6 is disabled. The interface cannot be in bridged mode. When you enable IPv6, the ACE automatically does the following:</p> <ul style="list-style-type: none"> <li>• Configures a link-local address (if not previously configured)</li> <li>• Performs duplicate address detection (DAD)</li> </ul> <p>Clear the check box to indicate that IPv6 is disabled on this interface.</p>                                                                                                                                                                                                                         |
| IPv6 Global Address  | <p>A global address is an IPv6 unicast address that is used for general IPv6 communication. Each global address is unique across the entire Internet. Therefore, its scope is global. The low order 64 bits can be assigned in several ways, including autoconfiguration using the EUI-64 format. You can configure only one globally unique IPv6 address on an interface.</p> <p>When you configure a global IPv6 address on an interface, the ACE automatically does the following:</p> <ul style="list-style-type: none"> <li>• Configures a link-local address (if not previously configured)</li> <li>• Performs duplicate address detection (DAD) on both addresses</li> </ul> |
| IPv6 Address         | <p>To configure an IPv6 global address on an interface, enter a complete IPv6 address with a prefix of 2000::/3 to 3fff::/3. For example, enter 2001:DB8:1::0.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p>                                                                                                                                                                                                                |

Table 10-3 VLAN Interface Attributes (continued)



| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alias IPv6 Address        | <p>When you configure redundancy with active and standby ACEs, you can configure a VLAN interface that has an alias global IPv6 address that is shared between the active and standby ACEs. The alias IPv6 address serves as a shared gateway for the two ACEs in a redundant configuration. You can configure only one alias global IPv6 address on an interface.</p> <p>To configure an IPv6 alias global address, enter a complete IPv6 address with a prefix of 2000::/3 to 3fff::/3. For example, enter 2001:DB8:1::0.</p>  <p><b>Note</b> You must configure redundancy (fault tolerance) on the ACE for the alias global IPv6 address to work.</p>                                                                                                                                                                                                                 |
| Peer IPv6 Address         | <p>To configure an IPv6 peer global address, enter a complete IPv6 address with a prefix of 2000::/3 to 3fff::/3. For example, enter 2001:DB8:1::0.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p>  <p><b>Note</b> The IPv6 peer global address must be unique across multiple contexts on a shared VLAN.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p> |
| Prefix Length             | <p>Enter the prefix length for all global addresses to specify how many of the most significant bits (MSBs) are used for the network identifier. Enter an integer from 3 to 127. If you use the optional EUI-64 check box for the global and peer addresses, the prefix must be less than or equal to 64.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IPv6 Unique-Local Address | <p>A unique local address is an optional IPv6 unicast address that is used for local communication within an organization and it is similar to a private IPv4 address (for example, 10.10.2.1). Unique local addresses have a global scope, but they are not routable on the internet, and they are assigned by a central authority. All unique local addresses have a predefined prefix of FC00::/7. You can configure only one IPv6 unique local address on an interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table 10-3 VLAN Interface Attributes (continued)




| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv6 Address            | <p>To configure a unique local address, enter a complete IPv6 address with an FC00::/7 prefix in the first field. In the second field after the /, enter the prefix length to specify how many of the most significant bits (MSBs) are used for the network identifier.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IPv6 Peer Address       | <p>In a redundant configuration, you can configure an IPv6 peer unique local address on the active that is synchronized to the standby ACE. You can configure only one peer unique local IPv6 address on an interface.</p> <p>To configure a peer unique local address, enter a complete IPv6 address with an FC00::/7 prefix in the first field. In the second field after the /, enter the prefix length to specify how many of the most significant bits (MSBs) are used for the network identifier.</p> <div>  <p><b>Note</b> The IPv6 peer unique local address must be unique across multiple contexts on a shared VLAN.</p> </div> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p> |
| Prefix Length           | <p>Enter the prefix length for all unique-local addresses to specify how many of the most significant bits (MSBs) are used for the network identifier. Enter an integer from 7 to 127. If you use the optional EUI-64 check box for the global and peer addresses, the prefix must be less than or equal to 64.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IPv6 Link-Local Address | <p>By default, when you enable IPv6 or configure a global IPv6 address on an interface, the ACE automatically creates a link local address for it. Every link local address must have a predefined prefix of FE80::/10. You can configure only one IPv6 link local address on an interface. This address always has the prefix of 64.</p> <p>To manually configure the link local address, enter a complete IPv6 address with an FE80::/10 prefix in this field. For example, enter FE80:DB8:1::1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Table 10-3 VLAN Interface Attributes (continued)

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv6 Peer Link-Local Address  | <p>In a redundant configuration, you can configure an IPv6 peer link local address for the standby ACE. You can configure only one peer link local address on an interface.</p> <p>To configure the peer link local address, enter a complete IPv6 address with an FE80::/10 prefix in this field.</p>  <p><b>Note</b> The IPv6 peer link local address must be unique across multiple contexts on a shared VLAN.</p>                                                                                                                          |
| <b>More Settings</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Enable ICMP Guard             | <p>Check the IPv4, IPv6 or both check boxes to indicate that ICMP Guard is to be enabled on the ACE appliance. Clear the check boxes to indicate that ICMP Guard is not to be enabled on ACE appliance.</p>  <p><b>Caution</b> Disabling ICMP security checks may expose your ACE appliance and network to potential security risks. When you disable ICMP Guard, the ACE appliance no longer performs NAT translations on the ICMP header and payload in error packets, which can potentially reveal real host IP addresses to attackers.</p> |
| Enable DHCP Relay             | <p>Check the IPv4, IPv6 or both check boxes to indicate that the ACE appliance is to accept DHCP requests from clients on this interface and to enable the DHCP relay agent.</p> <p>Clear the check boxes to indicate that the ACE appliance is not to accept DHCP requests or enable the DHCP relay agent.</p>                                                                                                                                                                                                                                                                                                                 |
| Reverse Path Forwarding (RPF) | <p>Check the IPv4, IPv6 or both check boxes to indicate that the ACE appliance is to discard IP packets if no reverse route is found or if the route does not match the interface on which the packets arrived.</p> <p>Clear the check boxes to indicate that the ACE appliance is not to filter or discard packets based on the ability to verify the source IP address.</p>                                                                                                                                                                                                                                                   |
| Reassembly Timeout (Seconds)  | <p>Enter the number of seconds that the ACE appliance is to wait before it abandons the fragment reassembly process if it doesn't receive any outstanding fragments for the current fragment chain (that is, fragments belonging to the same packet).</p> <ul style="list-style-type: none"> <li>For IPv4, valid entries are 1 to 30 seconds. The default is 5.</li> <li>For IPv6, valid entries are 1 to 60 seconds. The default is 60.</li> </ul>                                                                                                                                                                             |
| Max. Fragment Chains Allowed  | <p>Enter the maximum number of fragments belonging to the same packet that the ACE appliance is to accept for reassembly.</p> <p>For IPv4 and IPv6, valid entries are 1 to 256. The default is 24.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 10-3** *VLAN Interface Attributes (continued)*

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Min. Fragment MTU Value           | <p>Enter the minimum fragment size that the ACE appliance accepts for reassembly for a VLAN interface.</p> <ul style="list-style-type: none"> <li>For IPv4, valid entries are 28 to 9216 bytes. The default is 576.</li> <li>For IPv6, valid entries are 56 to 9216 bytes. The default is 1280.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                     |
| Action For IP Header Options      | <p>Select the IPv4, IPv6 or both action the ACE appliance is to take when an IP option is set in a packet:</p> <ul style="list-style-type: none"> <li>Allow—Indicates that the ACE appliance is to allow the IP packet with the IP options set.</li> <li>Clear—Indicates that the ACE appliance is to clear all IP options from the packet and to allow the packet.</li> <li>Clear-Invalid—Indicates that the ACE appliance is to clear the invalid IP options from the packet and then allow the packet. This action is the default for IPv4.</li> <li>Drop—Indicates that the ACE appliance is to discard the packet regardless of any options that are set. This action is the default for IPv6.</li> </ul> |
| Enable MAC Address Autogenerate   | Allows you to configure a different MAC address for the VLAN interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Min. TTL IP Header Value          | <p>Enter the minimum number of hops a packet is allowed to reach its destination. Valid entries are integers from 1 to 255. This field is applicable for IPv4 and IPv6 traffic.</p> <p>Each router along the packet's path decrements the TTL by one. If the packet's TTL reaches zero before the packet reaches its destination, the packet is discarded.</p>                                                                                                                                                                                                                                                                                                                                                 |
| MTU Value                         | Enter number of bytes for Maximum Transmission Units (MTUs). Valid entries are integers from 68 to 9216, and the default is 1500.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Enable Syn Cookie Threshold Value | Embryonic connection threshold above which the ACE applies SYN-cookie DoS protection. Valid entries are integers from 1 to 65535.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Action For DF Bit                 | <p>Indicate how the ACE appliance is to handle a packet that has its DF (Don't Fragment) bit set in the IP header:</p> <ul style="list-style-type: none"> <li>Allow—Indicates that the ACE appliance is to permit the packet with the DF bit set. If the packet is larger than the next-hop MTU, ACE appliance discards the packet and sends an ICMP unreachable message to the source host.</li> <li>Clear—Indicates that the ACE appliance is to clear the DF bit and permit the packet. If the packet is larger than the next-hop MTU, the ACE appliance fragments the packet.</li> </ul> <p>The default is Allow.</p>                                                                                      |




Table 10-3 VLAN Interface Attributes (continued)

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARP Inspection Type | <p>By default, ARP inspection is disabled on all interfaces, allowing all ARP packets through the ACE. When you enable ARP inspection, the ACE appliance uses the IPv4 address and interface ID (ifID) of an incoming ARP packet as an index into the ARP table. ARP inspection operates only on ingress bridged interfaces.</p> <p>ARP inspection prevents malicious users from impersonating other hosts or routers, known as ARP spoofing. ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router. The gateway router responds with the gateway router MAC address.</p> <p><b>Note</b> If ARP inspection fails, then the ACE does not perform source MAC validation.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> <li>• N/A—ARP inspection is disabled.</li> <li>• Flood—Enables ARP forwarding of nonmatching ARP packets. The ACE appliance forwards all ARP packets to all interfaces in the bridge group. This is the default setting. In the absence of a static ARP entry, this option bridges all packets.</li> <li>• No-flood—Disables ARP forwarding for the interface and drops nonmatching ARP packets. In the absence of a static ARP entry, this option does not bridge any packets.</li> </ul> |
| UDP Config Commands | <p>Select the UDP boost command:</p> <ul style="list-style-type: none"> <li>• N/A—not applicable</li> <li>• IP Destination Hash—Performs destination IP hash during connection.</li> <li>• IP Source Hash—Performs source IP hash during connection lookup.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table 10-3 VLAN Interface Attributes (continued)

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secondary IP Groups | <p>This option appears only when Interface Type is set to Routed.</p> <p>Enter a maximum of four secondary IP groups for the VLAN. The IP, alias IP, and peer IP addresses of each Secondary IP Group should be in the same subnet.</p> <p><b>Note</b> You cannot configure secondary IP addresses on FT VLANs.</p> <p>To create up to four secondary IP groups for the VLAN, do the following:</p> <ol style="list-style-type: none"> <li>Define one or more of the following secondary IP address types: <ul style="list-style-type: none"> <li>IP—Secondary IP address assigned to this interface. The primary address must be active for the secondary address to be active.</li> <li>AliasIP—Secondary IP address of the alias associated with this interface.</li> <li>PeerIP—Secondary IP address of the remote peer.</li> <li>Netmask—Secondary subnet mask to be used.</li> </ul> <p>The ACE has a system limit of 1,024 for each secondary IP address type.</p> </li> <li>Click <b>Add to selection</b> (right arrow) to add the group to the group display area.</li> <li>Repeat Steps 1 and 2 for each additional group.</li> <li>(Optional) Rearrange the order in which the groups are listed by selecting one of the group listings in the group display area and click either <b>Move item up in list</b> (up arrow) or <b>Move item down in list</b> (down arrow). Note that the ACE does not care what order the groups are in.</li> <li>(Optional) Edit a group or remove it from the list by selecting the desired group in the group display area and click <b>Remove from selection</b> (left arrow).</li> </ol> |
| Input Policies      | <p>From the Available list, double-click the policy map name that is associated with this VLAN interface or use the right arrow to move it to the Selected list. This policy map is to be applied to the inbound direction of the interface; that is, all traffic received by this interface.</p> <p>If you choose more than one policy map, use the Up and Down arrows to choose the priority of the policy map in the Selected list. These arrows modify the order of the policy maps for new VLANs only; they do not modify the policy map order when editing an existing policy map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Input Access Group  | <p>From the Available list, double-click an ACL name for the ACL input access group to be associated with this VLAN interface or use the right arrow to move it to the Selected list. Any ACL group listed in the Selected list specifies that this access group is to be applied to the inbound direction of the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 10-3 VLAN Interface Attributes (continued)

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Output Access Group               | From the Available list, double-click an ACL name for the ACL output access group that is associated with this VLAN interface or use the right arrow to move it to the Selected list. Any ACL group listed in the Selected list specifies that this access group is to be applied to the outbound direction of the interface; that is, all traffic sent by this interface.                                                                                                                                                                                                                                                                                                |
| Static ARP Entry (IP/MAC Address) | For the Static ARP entry, do the following: <ul style="list-style-type: none"> <li>a. In the ARP IP Address field, enter the IP address. This field accepts IPv4 addresses only.</li> <li>b. In the ARP MAC Address field, enter the hardware MAC address for the ARP table entry (for example, 00.02.9a.3b.94.d9).</li> <li>c. When completed, use the right arrow to move the static ARP entry to the list box. Use the Up and Down arrows to choose the priority of the static ARP entry in the list box. These arrows modify the order of the static ARPs for new VLANs only; they do not modify the static ARP order when editing an existing policy map.</li> </ul> |
| DHCP Relay Configuration          | Enter the IPv4 address of the DHCP server to which the DHCP relay agent is to forward client requests. Enter the IP address in dotted-decimal notation, such as 192.168.11.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| IPv6 Forward Interface VLAN       | Enter the VLAN to forward all received client requests with destination being the IPv6 DHCP address configured in the IPv6 DHCP Relay Configuration field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IPv6 DHCP Relay Configuration     | Enter the IPv6 address for the DHCP server where the DHCP relay agent forwards client requests.<br>Select the VLAN when the server address is a link local address.<br> <b>Note</b> When you enter a DHCPv6 server global IPv6 address, a VLAN is not required.                                                                                                                                                                                                                                                                                                                        |
| Managed-Config                    | Check the check box to indicate that the interface use the stateful autoconfiguration mechanism to configure IPv6 addresses.<br>Clear the check box to indicate that the interface does not use the stateful autoconfiguration mechanism to configure IPv6 addresses.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Other-Config                      | Check the check box to indicate that the interface use the stateful autoconfiguration mechanism to configure parameters other than IPv6 addresses.<br>Clear the check box to indicate that the interface does not use the stateful autoconfiguration mechanism to configure parameters other than IPv6 addresses.                                                                                                                                                                                                                                                                                                                                                         |

**Table 10-3** *VLAN Interface Attributes (continued)*

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NS Interval         | <p>The ACE sends neighbor solicitation messages through ICMPv6 on the local link to determine the IPv6 addresses of nearby nodes (hosts or routers). You can configure the rate at which the ACE sends these neighbor solicitation messages.</p> <p>By default, the interval at which the ACE sends NS messages for DAD default is 1000 milliseconds (msecs). To configure the interval, enter an integer from 1000 to 2147483647.</p>                                                    |
| NS Reachable Time   | <p>The neighbor solicitation reachable time is the time period in milliseconds during which a host considers the peer is reachable after a reachability confirmation from the peer. A reachability confirmation can include neighbor solicitation or advertisement, or any upper protocol traffic.</p> <p>By default, this time period is 0 milliseconds. To configure this time, enter an integer from 0 to 3600000.</p>                                                                 |
| Retransmission time | <p>By default, the advertised retransmission time is 0 milliseconds.</p> <p>To configure the retransmission time, enter an integer from 0 to 3600000.</p>                                                                                                                                                                                                                                                                                                                                 |
| DAD Attempts        | <p>By default, the number of attempts for sending duplicate address detection (DAD) is 1.</p> <p>To configure the DAD attempts, enter an integer from 0 to 255.</p>                                                                                                                                                                                                                                                                                                                       |
| RA Hop Limit        | <p>By default, the hop limit that neighbors should use when originating IPv6 packets is 64. To configure the hop limit in the IPv6 header, enter an integer from 0 to 255.</p>                                                                                                                                                                                                                                                                                                            |
| RA Lifetime         | <p>The router advertisement (RA) lifetime is the length of time that neighboring nodes should consider the ACE as the default router before they send RS messages again.</p> <p>By default, this length of time is 1800 seconds (30 minutes). To configure the RA lifetime, enter an integer from 0 to 9000.</p>                                                                                                                                                                          |
| RA Interval         | <p>By default, the rate at which the ACE sends RA messages is 600 seconds. To configure the rate, enter an integer from 4 to 1800. This interval must not exceed the RA lifetime.</p>                                                                                                                                                                                                                                                                                                     |
| Suppress RA         | <p>By default, the ACE automatically responds to RS messages that it receives from neighbors with RA messages that include, for example, the network prefix. You can instruct the ACE to not respond to RS messages.</p> <p>Check the check box to instruct the ACE to not respond to RS messages. The ACE also stops periodic unsolicited RAs that it sends at the RA interval.</p> <p>Clear the check box to reset the default behavior of automatically responding to RS messages.</p> |

**Table 10-3** *VLAN Interface Attributes (continued)*

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv6 Routing Prefix Advertisement | Click the Add button to configure the IPv6 prefixes that the ACE advertises in RA messages on the local link.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IPv6 Address/Prefix Length        | To configure IPv6 address advertised in the RA messages, enter a complete IPv6 address in the first field. In the second field after the /, enter the prefix length to specify how many of the most significant bits (MSBs) are used for the network identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| No Advertisements                 | Check the check box to indicate that the route prefix is not advertised.<br>Clear the check box to indicate that the route prefix is advertised.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Lifetime                          | Configure the prefix lifetime attributes as follows: <ul style="list-style-type: none"> <li>Lifetime Duration: <ul style="list-style-type: none"> <li>Valid Lifetime—By default, the prefix lifetime is 2592000 seconds (30 days). To configure the prefix lifetime in seconds, enter an integer from 0 to 2147183647.<br/>Select Infinite to indicate that the prefix never expires.</li> <li>Preferred Lifetime—By default, the prefix lifetime is 604800 seconds (10 days). To configure how long an IPv6 address remains preferred in seconds, enter an integer from 0 to 2147183647. This lifetime must not exceed the Valid Lifetime.<br/>Select Infinite to indicate that the preferred lifetime never expires.</li> </ul> </li> <li>Lifetime Expiration Date: <ul style="list-style-type: none"> <li>Valid Month/Day/Year/Time—Valid lifetime expiration date and time.</li> <li>Preferred Month/Day/Year/Time—Preferred lifetime expiration date and time.</li> </ul> </li> </ul> <p>Use the drop-down lists to select a day, month, and year. To specify the time, use the hh:mm format.</p> |
| Off-link:                         | This option appears when you enter a Preferred Lifetime field.<br>Check this check box to indicate that the route prefix is on a different subnet for a router to route to it.<br>Clear the check box to indicate that the route prefix is on the same subnet for a router to route to it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| No-autoconfig                     | This option appears when you enter a Preferred Lifetime field.<br>Check this check box to indicate to the host that it cannot use this prefix when creating an stateless IPv6 address.<br>Clear the check box to indicate to the host that it can use this prefix when creating an stateless IPv6 address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

- Step 4** Do the following:
- Click **Deploy Now** to save your entries and to return to the VLAN Interface table.
  - Click **Cancel** to exit the procedure without saving your changes and to return to the VLAN Interface table.
- Step 5** (Optional) To display statistics and status information for a VLAN interface, choose the VLAN interface from the VLAN Interface table, and then click **Details**.
- The **show interface vlan** CLI command output appears. See the “[Displaying VLAN Interface Statistics and Status Information](#)” section on page 10-23 for details.

#### Related Topic

- [Viewing All VLAN Interfaces, page 10-22](#)

## Viewing All VLAN Interfaces

Use this procedure to view all VLAN interfaces.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Network > VLAN Interfaces**.
- The VLAN Interface table appears listing all VLAN interfaces for the selected virtual context with the information shown in [Table 10-4](#).

**Table 10-4** *VLAN Interface Fields*

| Field              | Description                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN               | Name of the interface.                                                                                                                                                                                                                                                                                                                                 |
| Description        | Description for this interface.                                                                                                                                                                                                                                                                                                                        |
| Interface Type     | Role of the virtual context in the network topology of the VLAN interface: Routed, Bridged, or Unknown.                                                                                                                                                                                                                                                |
| IP Address         | IP address assigned to this interface including the netmask for an IPv4 address or a prefix length for an IPv6 address.<br><br>This table does not display the IPv6 link-local, unique-local, and multicast addresses for the interface. To display these addresses, click <b>Details</b> to display the output for the <b>show ipv6 vlan</b> command. |
| IPv6 Config Status | The status whether IPv6 is enabled or disabled on the interface.                                                                                                                                                                                                                                                                                       |
| Admin Status       | The status of the interface, which can be Up or Down.                                                                                                                                                                                                                                                                                                  |
| Operational Status | Operational state of the ACE (Up or Down).                                                                                                                                                                                                                                                                                                             |
| Last Polled        | Date and time of the last time that DM polled the ACE to display the current values.                                                                                                                                                                                                                                                                   |

**Related Topic**

- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)

## Displaying VLAN Interface Statistics and Status Information

You can display statistics and status information for a particular VLAN interface.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > Network > VLAN Interfaces**.  
The VLAN Interfaces table appears.
- Step 2** Choose a VLAN interface from the VLAN Interfaces table, and click **Details**.  
The **show interface vlan**, **show ipv6 vlan**, and **show ipv6 neighbors** CLI commands appears. Click on the command to display its output. For details on the displayed output fields, see the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.
- Step 3** Click **Close** to return to the VLAN Interfaces table.
- 


**Related Topics**

- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)

## Configuring Virtual Context BVI Interfaces

The ACE Appliance Device Manager supports virtual contexts containing Bridge-Group Virtual Interfaces (BVI). Use this procedure to configure BVI interfaces for virtual contexts.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > Network > BVI Interfaces**.  
The BVI Interface tables appears.
- Step 2** Click **Add** to add a new BVI interface, or select an existing BVI interface, and then click **Edit** to modify it.
-  **Note** If you click **Edit**, not all of the fields can be modified.
- 
- Step 3** Enter the interface attributes (see [Table 10-5](#)).

**Table 10-5** BVI Interface Attributes

| Field       | Description                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|
| BVI         | Either accept the automatically incremented entry or enter a different, unique value. Valid entries are integers from 1 to 4094. |
| Description | Enter a brief description for this interface.                                                                                    |

Table 10-5 BVI Interface Attributes (continued)


| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address                      | <p>Enter the IPv4 address assigned to this interface. This address must be a unique IP address that is not used in another context. Duplicate IP addresses in different contexts are not supported.</p> <p> <b>Note</b> If this interface is only used for IPv6 traffic, entering an IPv4 address is optional.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Alias IP Address                | Enter the IPv4 address of the alias this interface is associated with.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Peer IP Address                 | Enter the IPv4 address of the remote peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Netmask                         | Select the subnet mask to be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Enable MAC Address Autogenerate | Allows you to configure a different MAC address for the BVI interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Admin Status                    | Indicate whether you want the interface to be Up or Down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Secondary IP Groups             | <p>(Optional) Enter a maximum of four secondary IP groups for the BVI. To create up to four secondary IP groups for this BVI, do the following:</p> <ol style="list-style-type: none"> <li>Define one or more of the following secondary IP address types: <ul style="list-style-type: none"> <li>IP—Secondary IP address assigned to this interface. The primary address must be active for the secondary address to be active.</li> <li>AliasIP—Secondary IP address of the alias associated with this interface.</li> <li>PeerIP—Secondary IP address of the remote peer.</li> <li>Netmask—Secondary subnet mask to be used.</li> </ul> <p>The ACE has a system limit of 1,024 for each secondary IP address type.</p> </li> <li>Click Add to selection (right arrow) to add the group to the group display area.</li> <li>Repeat Steps 1 and 2 for each additional group.</li> <li>(Optional) Rearrange the order in which the groups are listed by selecting one of the group listings in the group display area and click either Move item up in list (up arrow) or Move item down in list (down arrow). Note that the ACE does not care what order the groups are in.</li> <li>(Optional) Edit a group or remove it from the list by selecting the desired group in the group display area and click Remove from selection (left arrow).</li> </ol> |
| First VLAN                      | Enter the first VLAN whose bridge group is to be configured with this BVI. This VLAN can be the server or client VLAN. Valid entries are from 2 to 4094.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| First VLAN Description          | Enter a brief description for the first VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



Table 10-5 BVI Interface Attributes (continued)


| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Second VLAN             | Enter the second VLAN whose bridge group is to be configured with this BVI. This VLAN can be the server or client VLAN. Valid entries are from 2 to 4094.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Second VLAN Description | Enter a brief description for the second VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Enable IPv6             | <p>Check the check box to enable IPv6 on this interface. By default, IPv6 is disabled. The interface cannot be in bridged mode. When you enable IPv6, the ACE automatically does the following:</p> <ul style="list-style-type: none"> <li>Configures a link-local address (if not previously configured)</li> <li>Performs duplicate address detection (DAD) on both addresses</li> </ul> <p>Clear the check box to indicate that IPv6 is disabled on this interface.</p>                                                                                                                                                                                  |
| IPv6 Global Address     | <p>A global address is an IPv6 unicast address that is used for general IPv6 communication. Each global address is unique across the entire Internet. Therefore, its scope is global. The low order 64 bits can be assigned in several ways, including autoconfiguration using the EUI-64 format. You can configure only one globally unique IPv6 address on an interface.</p> <p>When you configure a global address, the ACE automatically does the following:</p> <ul style="list-style-type: none"> <li>Configures a link-local address (if not previously configured)</li> <li>Performs duplicate address detection (DAD) on both addresses</li> </ul> |
| IPv6 Address            | <p>To configure an IPv6 global address on an interface, enter a complete IPv6 address with a prefix of 2000::/3 to 3fff::/3. For example, enter 2001:DB8:1::0.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p>                                                                                                                                                                                       |
| Alias IPv6 Address      | <p>When you configure redundancy with active and standby ACEs, you can configure a VLAN interface that has an alias global IPv6 address that is shared between the active and standby ACEs. The alias IPv6 address serves as a shared gateway for the two ACEs in a redundant configuration. You can configure only one alias global IPv6 address on an interface.</p> <p>To configure an IPv6 alias global address, enter a complete IPv6 address with a prefix of 2000::/3 to 3fff::/3. For example, enter 2001:DB8:1::0.</p>                                                                                                                             |
|                         |  <p><b>Note</b> You must configure redundancy (fault tolerance) on the ACE for the alias global IPv6 address to work.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Table 10-5 BVI Interface Attributes (continued)


| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Peer IPv6 Address         | <p>To configure an IPv6 peer global address, enter a complete IPv6 address with a prefix of 2000::/3 to 3fff::/3. For example, enter 2001:DB8:1::0.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p> <div>  <p><b>Note</b> The IPv6 peer global address must be unique across multiple contexts on a shared VLAN.</p> </div> |
| Prefix Length             | <p>Enter the prefix length for all global addresses to specify how many of the most significant bits (MSBs) are used for the network identifier. Enter an integer from 3 to 127. If you use the optional EUI-64 check box for the global and peer addresses, the prefix must be less than or equal to 64.</p>                                                                                                                                                                                                                                                                                                                                                       |
| IPv6 Unique-Local Address | <p>A unique local address is an optional IPv6 unicast address that is used for local communication within an organization and it is similar to a private IPv4 address (for example, 10.10.2.1). Unique local addresses have a global scope, but they are not routable on the internet, and they are assigned by a central authority. All unique local addresses have a predefined prefix of FC00::/7. You can configure only one IPv6 unique local address on an interface.</p>                                                                                                                                                                                     |
| IPv6 Address              | <p>To configure a unique local address, enter a complete IPv6 address with an FC00::/7 prefix in the first field. In the second field after the /, enter the prefix length to specify how many of the most significant bits (MSBs) are used for the network identifier.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p>                                                                                      |

Table 10-5 BVI Interface Attributes (continued)



| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Peer IPv6 Address            | <p>In a redundant configuration, you can configure an IPv6 peer unique local address on the active that is synchronized to the standby ACE. You can configure only one peer unique local IPv6 address on an interface.</p> <p>To configure a peer unique local address, enter a complete IPv6 address with an FC00::/7 prefix in the first field. In the second field after the /, enter the prefix length to specify how many of the most significant bits (MSBs) are used for the network identifier.</p> <p></p> <p><b>Note</b> The IPv6 peer unique local address must be unique across multiple contexts on a shared VLAN.</p> <p>Check the EUI-64 box to specify that the low order 64 bits are automatically generated in the IEEE 64-bit Extended Unique Identifier (EUI-64) format specified in RFC 2373. To use EUI-64, the Prefix Length field must be less than or equal to 64 and the host segment must be all zeros.</p> |
| Prefix Length                | <p>Enter the prefix length for all global addresses to specify how many of the most significant bits (MSBs) are used for the network identifier. Enter an integer from 7 to 127. If you use the optional EUI-64 check box for the global and peer addresses, the prefix must be less than or equal to 64.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IPv6 Link-Local Address      | <p>By default, when you enable IPv6 or configure any other valid IPv6 address on an interface, the ACE automatically creates a link local address for it. Every link local address must have a predefined prefix of FE80::/10. You can configure only one IPv6 link local address on an interface. This address always has the prefix of 64.</p> <p>To manually configure the link local address, enter a complete IPv6 address with an FE80::/10 prefix in this field. For example, enter FE80:DB8:1::1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IPv6 Peer Link-Local Address | <p>In a redundant configuration, you can configure an IPv6 peer link local address for the standby ACE. You can configure only one peer link local address on an interface.</p> <p>To configure the peer link local address, enter a complete IPv6 address with an FE80::/10 prefix in this field.</p> <p></p> <p><b>Note</b> The IPv6 peer link local address must be unique across multiple contexts on a shared VLAN.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>More Settings</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Managed-Config               | <p>Check the check box to indicate that the interface use the stateful autoconfiguration mechanism to configure IPv6 addresses.</p> <p>Clear the check box to indicate that the interface does not use the stateful autoconfiguration mechanism to configure IPv6 addresses.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Table 10-5 BVI Interface Attributes (continued)

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Other-Config        | <p>Check the check box to indicate that the interface use the stateful autoconfiguration mechanism to configure parameters other than IPv6 addresses.</p> <p>Clear the check box to indicate that the interface does not use the stateful autoconfiguration mechanism to configure parameters other than IPv6 addresses.</p>                                                                                                           |
| NS Interval         | <p>The ACE sends neighbor solicitation messages through ICMPv6 on the local link to determine the IPv6 addresses of nearby nodes (hosts or routers). You can configure the rate at which the ACE sends these neighbor solicitation messages.</p> <p>By default, the interval at which the ACE sends NS messages for DAD default is 1000 milliseconds (msecs). To configure the interval, enter an integer from 1000 to 2147483647.</p> |
| NS Reachable Time   | <p>The neighbor solicitation reachable time is the time period in milliseconds during which a host considers the peer is reachable after a reachability confirmation from the peer. A reachability confirmation can include neighbor solicitation or advertisement, or any upper protocol traffic.</p> <p>By default, this time period is 0 milliseconds. To configure this time, enter an integer from 0 to 3600000.</p>              |
| Retransmission time | <p>By default, the advertised retransmission time is 0 milliseconds.</p> <p>To configure the retransmission time, enter an integer from 0 to 3600000.</p>                                                                                                                                                                                                                                                                              |
| DAD Attempts        | <p>By default, the number of attempts for sending duplicate address detection (DAD) is 1.</p> <p>To configure the DAD attempts, enter an integer from 0 to 255.</p>                                                                                                                                                                                                                                                                    |
| RA Hop Limit        | <p>By default, the hop limit that neighbors should use when originating IPv6 packets is 64. To configure the hop limit in the IPv6 header, enter an integer from 0 to 255.</p>                                                                                                                                                                                                                                                         |
| RA Lifetime         | <p>The router advertisement (RA) lifetime is the length of time that neighboring nodes should consider the ACE as the default router before they send RS messages again.</p> <p>By default, this length of time is 1800 seconds (30 minutes). To configure the RA lifetime, enter an integer from 0 to 9000.</p>                                                                                                                       |
| RA Interval         | <p>By default, the rate at which the ACE sends RA messages is 600 seconds. To configure the rate, enter an integer from 4 to 1800. This interval must not exceed the RA lifetime.</p>                                                                                                                                                                                                                                                  |

Table 10-5 BVI Interface Attributes (continued)

| Field                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Suppress RA                       | <p>By default, the ACE automatically responds to RS messages that it receives from neighbors with RA messages that include, for example, the network prefix.</p> <p>Check the check box to instruct the ACE to not respond to RS messages. The ACE also stops periodic unsolicited RAs that it sends at the RA interval.</p> <p>Clear the check box to reset the default behavior of automatically responding to RS messages.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| IPv6 Routing Prefix Advertisement | Click the Add button to configure the IPv6 prefixes that the ACE advertises in RA messages on the local link.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IPv6 Address/Prefix Length        | To configure IPv6 address advertised in the RA messages, enter a complete IPv6 address in the first field. In the second field after the /, enter the prefix length to specify how many of the most significant bits (MSBs) are used for the network identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| No Advertisements                 | <p>Check the check box to indicate that the route prefix is not advertised.</p> <p>Clear the check box to indicate that the route prefix is advertised.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Lifetime                          | <p>Configure the prefix lifetime attributes as follows:</p> <ul style="list-style-type: none"> <li>• Lifetime Duration: <ul style="list-style-type: none"> <li>– Valid Lifetime—By default, the prefix lifetime is 2592000 seconds (30 days). To configure the prefix lifetime in seconds, enter an integer from 0 to 2147183647.</li> <li>Select Infinite to indicate that the prefix never expires.</li> <li>– Preferred Lifetime—By default, the prefix lifetime is 604800 seconds (10 days). To configure how long an IPv6 address remains preferred in seconds, enter an integer from 0 to 2147183647. This lifetime must not exceed the Valid Lifetime.</li> <li>Select Infinite to indicate that the preferred lifetime never expires.</li> </ul> </li> <li>• Lifetime Expiration Date: <ul style="list-style-type: none"> <li>– Valid Month/Day/Year/Time—Valid lifetime expiration date and time.</li> <li>– Preferred Month/Day/Year/Time—Preferred lifetime expiration date and time.</li> </ul> </li> </ul> <p>Use the drop-down lists to select a day, month, and year. To specify the time, use the hh:mm format.</p> |

**Table 10-5** *BVI Interface Attributes (continued)*

| Field         | Description                                                                                                                                                                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Off-link:     | <p>This option appears when you enter a Preferred Lifetime field.</p> <p>Check this check box to indicate that the route prefix is on a different subnet for a router to route to it.</p> <p>Clear the check box to indicate that the route prefix is on the same subnet for a router to route to it.</p>                 |
| No-autoconfig | <p>This option appears when you enter a Preferred Lifetime field.</p> <p>Check this check box to indicate to the host that it cannot use this prefix when creating an stateless IPv6 address.</p> <p>Clear the check box to indicate to the host that it can use this prefix when creating an stateless IPv6 address.</p> |

**Step 4** Do the following:

- Click **Deploy Now** to save your entries and to return to the BVI Interface table.
- Click **Cancel** to exit the procedure without saving your entries and to return to the BVI Interface table.

**Step 5** To display statistics and status information for a BVI interface, choose the BVI interface from the BVI Interface table, and click **Details**.

The **show interface bvi**, **show ipv6 interface bvi**, and **show ipv6 neighbors** CLI commands appear. See the “[Displaying BVI Interface Statistics and Status Information](#)” section on page 10-31 for details.

#### Related Topics

- [Configuring Network Access, page 10-1](#)
- [Configuring Virtual Context Primary Attributes, page 4-11](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring Traffic Policies, page 12-1](#)

## Viewing All BVI Interfaces by Context

To view all BVI interfaces associated with a specific virtual context, select **Config > Virtual Contexts > context > Network > BVI Interfaces**.

The BVI Interface table appears with the information shown in [Table 10-6](#).

**Table 10-6** *BVI Interface Fields*

| Field       | Description                     |
|-------------|---------------------------------|
| BVI         | Name of the interface.          |
| Description | Description for this interface. |

Table 10-6 BVI Interface Fields

| Field              | Description                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------|
| IP Address         | IP address assigned to this interface including the netmask for an IPv4 address or a prefix length for an IPv6 address. |
| IPv6 Config Status | The status whether IPv6 is enabled or disabled on the interface.                                                        |
| Admin Status       | The status of the interface, which can be Up or Down.                                                                   |
| Operational Status | Operational state of the ACE (Up or Down).                                                                              |
| Last Polled Time   | Date and time of the last time that DM polled the ACE to display the current values.                                    |

**Related Topics**

- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Using Virtual Contexts, page 4-2](#)
- [Configuring Virtual Context Primary Attributes, page 4-11](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context Syslog Logging, page 4-12](#)
- [Configuring Traffic Policies, page 12-1](#)

## Displaying BVI Interface Statistics and Status Information

You can display statistics and status information for a particular BVI interface by using the **Details** button. DM accesses the **show interface bvi**, **show ipv6 interface bvi**, and **show ipv6 neighbors** CLI commands to display detailed BVI interface information.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > Network > BVI Interfaces**.  
The BVI Interface table appears.
- Step 2** In the BVI Interface table, choose a BVI interface from the BVI Interface table, and click **Details**.  
The **show interface bvi**, **show ipv6 interface bvi**, and **show ipv6 neighbors** CLI commands appear. Click on the command to display its output. For details on the displayed output fields, see the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.
- Step 3** Click **Close** to return to the BVI Interface table.
- 

**Related Topics**

- [Viewing All BVI Interfaces by Context, page 10-30](#)

# Configuring VLAN Interface NAT Pools and Displaying NAT Utilization

You can configure Network Address Translation (NAT) pools, which are designed to simplify and conserve IP addresses. A NAT pool allows private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before the packets are forwarded to another network.

In addition to creating a NAT pool, you can display the utilization information associated with it.

This section includes the following topics:

- [Configuring VLAN Interface NAT Pools, page 10-32](#)
- [Displaying NAT Pool Utilization, page 10-33](#)

## Configuring VLAN Interface NAT Pools

This procedure shows how to configure NAT pools for a VLAN interface.

### Guidelines and Restrictions

- The ACE Appliance Device Manager allows you to configure NAT so that it advertises only one address for the entire network to the outside world. This effectively hides the entire internal network behind that address, thereby offering both security and address conservation.
- Several internal addresses can be translated to only one or a few external addresses by using Port Address Translation (PAT) in conjunction with NAT. With PAT, you can configure static address translations at the port level and use the remainder of the IP address for other translations. PAT effectively extends NAT from one-to-one to many-to-one by associating the source port with each flow.
- When server load balancing is IPv6 to IPv4 or IPv4 to IPv6, you must configure source NAT.

### Prerequisites

At least one VLAN interface is configured on the ACE (see [Configuring Virtual Context VLAN Interfaces, page 10-10](#)).

### Procedure

- 
- |               |                                                                                                                                                                                                                                                    |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; <i>virtual_context</i> &gt; Network &gt; NAT Pools</b> .<br>The NAT Pools table appears.                                                                                                               |
| <b>Step 2</b> | In the NAT Pools table, click <b>Add</b> to add a new entry. The NAT Pool configuration screen appears.                                                                                                                                            |
| <b>Step 3</b> | Select the VLAN interface you want to configure a NAT pool.                                                                                                                                                                                        |
| <b>Step 4</b> | In the NAT Pool Id field, either accept the automatically incremented entry or enter a new number to uniquely identify this pool. Valid entries are integers from 1 to 2147483647.                                                                 |
| <b>Step 5</b> | For the IP Address Type, select either IPv4 or IPv6.                                                                                                                                                                                               |
| <b>Step 6</b> | In the Start IP Address field, enter an IP address for the selected IP Address Type. This entry identifies either a single IP address or, if using a range of IP addresses, the first IP address in a range of global addresses for this NAT pool. |



- Step 7** In the End IP Address field, enter the highest IP address in a range of global IP addresses for this NAT pool. Enter the IP address for the selected IP Address Type.
- Leave this field blank if you want to identify only the single IP address in the Start IP Address field.
- Step 8** In the Netmask field for an IPv4 address, select the subnet mask for the global IP addresses in the NAT pool. In the Prefix Length field for an IPv6 address, enter the prefix length for the global IP addresses in the NAT pool.
- Step 9** Check the PAT Enabled check box to indicate that the ACE appliance is to perform port address translation (PAT) in addition to NAT. Clear the check box to indicate that the ACE appliance is not to perform port address translation (PAT) in addition to NAT.
- Step 10** Do the following:
- Click **Deploy Now** to save your entries and to return to the NAT Pool table.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the NAT Pool table.
  - Click **Next** to save your entries and to add another NAT Pool entry.
- 

#### Related Topics

- [Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32](#)
- [Displaying NAT Pool Utilization, page 10-33](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)
- [Configuring Virtual Context BVI Interfaces, page 10-23](#)

## Displaying NAT Pool Utilization

This procedure shows how to display the utilization of all configured NAT pools on all VLANs.

#### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > *virtual\_context* > Network > NAT Pools**.
- The NAT Pools table appears.
- Step 2** Click **Show NAT Pool Utilization**.
- The **show nat-fabric nat-pool-utilization** command pop-up window appears, displaying the following information:
- Pool ID—Unique NAT pool identifier.
  - NP—ACE network processor to which the NAT is bound.
  - Total/Usage/Utilization (%):
    - Total—Number of IP addresses configured in the NAT pool.
    - Usage—Number of IP addresses being used.
    - Utilization (%)—Percentage of configured IP addresses be used.
  - LowerIP/UpperIP—Lower and upper IP addresses configured in the NAT pool IP address range.
  - Context—Context to which the NAT pool belongs.

- Step 3** From the pop-up window, do one of the following:
- Click **Update Details** to refresh the information displayed.
  - Click **Close** to close the pop-up window.

#### Related Topics

- [Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32](#)
- [Configuring VLAN Interface NAT Pools, page 10-32](#)

## Configuring Virtual Context Static Routes

Admin and user context modes do not support dynamic routing, therefore you must use static routes for any networks to which the ACE appliance is not directly connected, such as when there is a router between a network and the ACE appliance.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Network > Static Routes**.

The Static Route table appears.

- Step 2** To add a static route for this context, click **Add**.



**Note** You cannot modify an existing static route. To make changes to an existing static route, you must delete the static route and then add it back.

- Step 3** For the IP Address Type, select either IPv4 or IPv6 for the route.

- Step 4** In the Destination Prefix field, enter the IP address based on the address type (IPv4 or IPv6) for the route. The address you specify for the static route is the address that is in the packet before entering the ACE appliance and performing network address translation.

- Step 5** In the Destination Prefix Mask field for an IPv4 address, select the subnet to use for this route.

In the Destination Prefix-length field for an IPv6 address, enter the prefix length from 0 to 128 to use for this route.

- Step 6** (IPv6 IP Address Type only) For the Outgoing Interface Type, select one of the following:

- N/A (Not applicable)
- VLAN
- BVI

If you select VLAN or BVI, select its number from the drop down menu. To configure an interface, click **Plus**. After configuring it, select its number from the drop down menu.

- Step 7** In the Next Hop field, enter the IP address of the gateway router based on the address type (IPv4 or IPv6) for this route. The gateway address must be in the same network as a VLAN interface for this context.

- Step 8** Do the following:

- Click **Deploy Now** to save your entries and to return to the Static Route table.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Static Route table.
  - Click **Next** to save your entries and to add another static route.
- 

**Related Topics**

- [Configuring Virtual Contexts, page 4-7](#)
- [Configuring Virtual Context Primary Attributes, page 4-11](#)
- [Managing ACE Appliance Licenses, page 4-29](#)
- [Configuring High Availability, page 11-1](#)

## Viewing All Static Routes by Context

Use this procedure to view all static routes associated with a virtual context.

**Procedure**

---

**Step 1** Choose **Config > Virtual Contexts > context > Network > Static Routes**.

The Static Route table appears with the following information:

- Destination prefix address
  - Destination prefix mask or prefix length
  - Next hop IP address
- 

**Related Topics**

- [Configuring Virtual Context Static Routes, page 10-34](#)
- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)

## Configuring Global IP DHCP

DM can configure the DHCP relay agent on the ACE. When you configure the ACE as a DHCP relay agent, it is responsible for forwarding the requests and responses that are negotiated between the DHCP clients and the server. By default, the DHCP relay agent is disabled. You must configure a DHCP server when you enable the DHCP relay agent.

The following steps show you how to configure the DHCP relay agent at the context level so the configuration applies to all interfaces associated with the context.

**Note**

The options that appear when you select **Config > Virtual Contexts > context** depend on the device associated with the virtual context and the role associated with your account.

---

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Network > Global IP DHCP**. The Global IP DHCP configuration table appears.
- Step 2** For **Enable DHCP Relay For The Context**, click IPv4, IPv6 or both to enable DHCP relay for the context and all interfaces associated with this context.
- Step 3** Select a relay agent information forwarding policy, as follows:
- N/A—Specifies to not configure the DHCP relay to identify what is to be performed if a forwarded message already contains relay information.
  - Keep—Specifies that existing information is left unchanged on the DHCP relay agent.
  - Replace—Specifies that existing information is overwritten on the DHCP relay agent.
- Step 4** In the IP DHCP Server field, select the IP DHCP server to which the DHCP relay agent is to forward client requests.
- Step 5** In the IPv6 Forward Interface VLAN field, you can optionally enter the VLAN interface number that you configured in the [IPv6 Forward Interface VLAN](#) field on the interface where the multicast DHCP relay message is sent.
- Step 6** In the IPv6 DHCP server, specify one or more IP DHCP servers and IPv6 addresses to which the DHCP relay agent is to forward client requests.
- Step 7** Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- 

### Related Topics

- [Configuring Virtual Context VLAN Interfaces, page 10-10](#)



# CHAPTER 11

## Configuring High Availability

---

This chapter describes how to configure high availability. High Availability (or fault tolerance) uses a maximum of two ACE appliances to ensure that your network remains operational even if one of the appliances becomes unresponsive. Redundancy ensures that your network services and applications are always available.



**Note**

---

Redundancy is not supported between an ACE appliance and an ACE module operating as peers. Redundancy must be of the same ACE device type and software release.

---



**Note**

---

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

### Related Topics

- [Understanding ACE Redundancy, page 11-2](#)
- [Configuring ACE High Availability, page 11-8](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Switching Over a High Availability Group, page 11-16](#)
- [Deleting ACE High Availability Groups, page 11-17](#)
- [High Availability Tracking and Failure Detection Overview, page 11-17](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)
- [Tracking Hosts for High Availability, page 11-20](#)
- [Configuring Host Tracking Probes, page 11-21](#)
- [Configuring Peer Host Tracking Probes, page 11-22](#)

# Understanding ACE Redundancy

Redundancy provides seamless switchover of flows in case an ACE appliance becomes unresponsive or a critical host or interface fails. Redundancy supports the following network applications that require fault tolerance:

- Mission-critical enterprise applications
- Banking and financial services
- E-commerce
- Long-lived flows such as FTP and HTTP file transfers

The following overview topics describe high availability as performed by the ACE appliance:

- [High Availability Polling, page 11-2](#)
- [Redundancy Protocol, page 11-3](#)
- [Stateful Failover, page 11-4](#)
- [Fault-Tolerant VLAN, page 11-5](#)
- [Configuration Synchronization, page 11-5](#)
- [Synchronizing High Availability Configurations with ACE Appliance Device Manager, page 11-6](#)
- [Redundancy Configuration Requirements and Restrictions, page 11-6](#)

## Related Topics

- [Configuring ACE High Availability, page 11-8](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)

## High Availability Polling

Approximately every two minutes, the ACE appliance Device Manager issues the **show ft group** command to the ACE appliance to gather the redundancy statistics of each virtual context. The state information is displayed in the HA State and HA Peer State fields when you click **Config > Virtual Context**. The possible states are as follows:

- Active—Local member of the FT group is active and processing flows.
- Standby Cold—Indicates if the FT VLAN is down but the peer device is still alive, or the configuration or application state synchronization failed. When a context is in this state and a switchover occurs, the transition to the ACTIVE state is stateless.
- Standby Bulk—Local standby context is waiting to receive state information from its active peer context. The active peer context receives a notification to send a snapshot of the current state information for all applications to the standby context.
- Standby Hot—Local standby context has all the state information it needs to statefully assume the active state if a switchover occurs.
- Standby Warm—Allows the configuration and state synchronization process to continue on a best-effort basis when you upgrade or downgrade the ACE software.
- N/A—Indicates that the ACE Device Manager received an empty state from the ACE which can occur during a transition period between state changes, for example, during a switchover.

**Note**

When you upgrade or downgrade the ACE from one software version to another, there is a point in the process when the two ACEs have different software versions and, therefore, a software incompatibility. When the Standby Warm state appears, this means that the active ACE will continue to synchronize configuration and state information to the standby even though the standby may not recognize or understand the software commands or state information. This standby state allows the standby ACE to come up with best-effort support.

## Redundancy Protocol

You can configure a maximum of two ACE appliances (peers) for redundancy. Each peer appliance can contain one or more fault-tolerant (FT) groups. Each FT group consists of two members: one active context and one standby context. An FT group has a unique group ID that you assign.

**Note**

For the replication process to function properly and successfully replicate the configuration for a user context when switching from the active context to the standby context, ensure that each user context has been added to the FT group. All applicable user contexts must be part of an FT group for redundancy to function properly.

One virtual MAC address (VMAC) is associated with each FT group. The format of the VMAC is 00-0b-fc-fe-1b-*groupID*. Because a VMAC does not change upon switchover, the client and server ARP tables does not require updating. The ACE selects a VMAC from a pool of virtual MACs available to it. For more information, see [Configuring Virtual Contexts, page 4-7](#).

Each FT group acts as an independent redundancy instance. When a switchover occurs, the active member in the FT group becomes the standby member and the original standby member becomes the active member. A switchover can occur for the following reasons:

- The active member becomes unresponsive.
- A tracked host or interface fails.
- You force a switchover for a high availability group by clicking **Switchover** in the ACE HA Groups table (see [Switching Over a High Availability Group, page 11-16](#)).

To outside nodes (clients and servers), the active and standby FT group members appear as one node with respect to their IP addresses and associated VMAC. The ACE provides active-active redundancy with multiple contexts only when there are multiple FT groups configured on each appliance and both appliances contain at least one active group member (context). With a single context, the ACE supports active-backup redundancy and each group member is an Admin context.

The ACE sends and receives all redundancy-related traffic (protocol packets, configuration data, heartbeats, and state replication packets) on a dedicated FT VLAN. You cannot use this dedicated VLAN for normal traffic.

To optimize the transmission of heartbeat packets for multiple FT groups and to minimize network traffic, the ACE sends and receives heartbeat messages using a separate process. The ACE uses the heartbeat to probe the peer ACE, rather than probe each context. When an ACE does not receive a heartbeat from the peer ACE, all the contexts in the standby state become active. The ACE sends heartbeat packets over UDP. You can set the frequency with which the ACE sends heartbeat packets as part of the FT peer configuration. For details about configuring the heartbeat, see [Configuring High Availability Peers, page 11-8](#).

The election of the active member within each FT group is based on a priority scheme. The member configured with the higher priority is elected as the active member. If a member with a higher priority is found after the other member becomes active, the new member becomes active because it has a higher priority. This behavior is known as preemption and is enabled by default. You can override this default behavior by disabling preemption. To disable preemption, use the `Preempt` parameter. Enabling `Preempt` causes the member with the higher priority to assert itself and become active. For details about configuring preemption, see [Configuring ACE High Availability Groups, page 11-11](#).

## Stateful Failover

The ACE replicates flows on the active FT group member to the standby group member per connection for each context. The replicated flows contain all the flow-state information necessary for the standby member to take over the flow if the active member becomes unresponsive. If the active member becomes unresponsive, the replicated flows on the standby member become active when the standby member assumes mastership of the context. The active flows on the former active member transition to a standby state to fully back up the active flows on the new active member.

**Note**

For the replication process to function properly and successfully replicate the configuration for a user context when switching from the active context to the standby context, ensure that each user context has been added to the FT group. All applicable user contexts must be part of an FT group for redundancy to function properly.

**Note**

By default, connection replication is enabled in the ACE appliance.

After a switchover occurs, the same connection information is available on the new active member. Supported end-user applications do not need to reconnect to maintain the same network session.

The state information passed to the standby appliance includes the following data:

- Network Address Translation (NAT) table based on information synchronized with the connection record
- All Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections not terminated by the ACE appliance
- HTTP connection states (Optional)
- Sticky table

**Note**

In a user context, the ACE appliance allows a switchover only of the FT group that belongs to that context. In the Admin context, the ACE appliance allows a switchover of all FT groups in all configured contexts in the appliance.

To ensure that bridge learning occurs quickly upon a switchover in a Layer 2 configuration in the case where a VMAC moves to a new location, the new active member sends a gratuitous ARP on every interface associated with the active context. Also, when there are two VLANs on the same subnet and servers need to send packets to clients directly, the servers must know the location of the gateway on the client-side VLAN. The active member acts as the bridge for the two VLANs. In order to initiate learning of the new location of the gateway, the new active member sends an ARP request to the gateway on the client VLAN and bridges the ARP response onto the server VLAN.



## Fault-Tolerant VLAN

Redundancy uses a dedicated fault-tolerant VLAN between redundant ACEs to transmit flow-state information and the redundancy heartbeat. Do not use this dedicated VLAN for normal network traffic. You must configure this same VLAN on both peer ACEs. You also must configure a different IP address within the same subnet on each ACE for the fault-tolerant VLAN.

The two redundant ACEs constantly communicate over the fault-tolerant VLAN to determine the operating status of each ACE. The standby member uses the heartbeat packet to monitor the health of the active member. The active member uses the heartbeat packet to monitor the health of the standby member. Communications over the switchover link include the following data:

- Redundancy protocol packets
- State information replication data
- Configuration synchronization information
- Heartbeat packets

For multiple contexts, the fault-tolerant VLAN resides in the system configuration data. Each fault-tolerant VLAN on the ACE has one unique MAC address associated with it. The ACE uses these device MAC addresses as the source or destination MACs for sending or receiving redundancy protocol state and configuration replication packets.



**Note**

---

The IP address and the MAC address of the fault-tolerant VLAN do not change at switchover.

---

## Configuration Synchronization

For redundancy to function properly, both members of an fault-tolerant group must have identical configurations. Ensure that both ACE appliances include the same bandwidth software license (2G or 1G) and the same virtual context software license. If there is a mismatch in software license between the two ACE appliances in an FT group, the following operational behavior can occur:

- If there is a mismatch in virtual context software license, synchronization between the active ACE and standby ACE may not work properly.
- If both the active and the standby ACE appliances have the same virtual content software license but have a different bandwidth software license, synchronization will work properly but the standby ACE may experience a potential loss of traffic on switchover from the 2G ACE appliance to the 1G ACE appliance.

See the *Administration Guide, Cisco ACE Application Control Engine* for details about the available ACE software licenses.

The ACE automatically replicates the active configuration on the standby member using a process called *configuration synchronization* (config sync). Config sync automatically replicates any changes made to the configuration of the active member to the standby member. After the ACE synchronizes the redundancy configuration from the active member to the standby peer, it disables configuration mode on the standby. See [Synchronizing High Availability Configurations with ACE Appliance Device Manager](#), page 11-6.

## Synchronizing High Availability Configurations with ACE Appliance Device Manager

When two ACE appliances are configured as high availability peers, their configurations must be synchronized at all times so that the standby ACE peer can seamlessly take over for the active ACE peer. As the active and standby ACEs synchronize, the configuration on the standby ACE appliance can become out of synchronization with the ACE Appliance Device Manager-maintained configuration data for that ACE appliance.

When an ACE appliance is in a standby state, if you make configuration changes on the active ACE appliance this change is also synchronized with the standby ACE appliance. However, when you access the Device Manager GUI you will not observe the configuration changes on the standby ACE. Yet, if you access the CLI on the standby ACE and display redundancy configurations using the **show running-config ft** command in Exec mode, you will see these configuration changes.

As a result, it is important for you to manually synchronize the ACE Appliance Device Manager on the standby appliance to observe the entire configuration. See the [“Manually Synchronizing Individual Virtual Context Configurations” section on page 4-82](#).

When the ACE appliance performs a context failover (proceeds from the Standby Warm state or Standby Hot state) to the Active state), the new active ACE appliance auto-synchronizes the configuration and updates the ACE appliance Device Manager GUI.

In a high availability pair, the two configured virtual contexts synchronize with each other as part of their ongoing communications. However, their copies do not synchronize in ACE Appliance Device Manager and the configuration on the standby member can become out of sync with the configuration on the ACE appliance.

After the active member of a high availability pair fails and the standby member becomes active, ACE Appliance Device Manager on the newly active member detects any out-of-sync virtual context configurations and reports that status in the All Virtual Contexts table so that you can synchronize the virtual context configurations.

For information on synchronizing some or all virtual context configurations, see the following topics:

- [Manually Synchronizing Individual Virtual Context Configurations, page 4-82](#)
- [Manually Synchronizing All Virtual Context Configurations, page 4-83](#)

### Related Topics

- [High Availability Polling, page 11-2](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Manually Synchronizing Individual Virtual Context Configurations, page 4-82](#)
- [Manually Synchronizing All Virtual Context Configurations, page 4-83](#)

## Redundancy Configuration Requirements and Restrictions

Follow these requirements and restrictions when configuring the redundancy feature.

- In bridged mode (Layer 2), two contexts cannot share the same VLAN.
- To achieve active-active redundancy, a minimum of two contexts and two fault-tolerant groups are required on each ACE.

- When you configure redundancy, the ACE keeps all interfaces that do not have an IP address in the Down state. The IP address and the peer IP address that you assign to a VLAN interface should be in the same subnet, but different IP addresses. For more information about configuring VLAN interfaces, see [Configuring Virtual Context VLAN Interfaces, page 10-10](#).
- In a high availability pair, the two configured virtual contexts synchronize with each other as part of their ongoing communications. However, their copies do not synchronize in ACE Appliance Device Manager and the configuration on the standby member can become out of sync with the configuration on the ACE appliance. After the active member of a high availability pair fails and the standby member becomes active, ACE Appliance Device Manager on the newly active member detects any out-of-sync virtual context configurations and reports that status in the All Virtual Contexts table so that you can synchronize the virtual context configurations.
- When a virtual context is in either the Standby Hot or Standby Warm state (see [High Availability Polling, page 11-2](#)), the virtual context may receive configuration changes from its ACE peer without updating the Device Manager GUI. As a result, the ACE appliance Device Manager GUI will be out of synchronization with the CLI configuration. If you need to check configuration on a standby virtual context using the tracking and failure detection process (see [Tracking VLAN Interfaces for High Availability, page 11-19](#)), we recommend that you first perform a manual synchronization using either the CLI Sync or CLI Sync All buttons before checking the configuration values.

# Configuring ACE High Availability

The tasks involved with configuring high availability are described in [Table 11-1](#).

**Table 11-1** High Availability Task Overview

|        | Task                                                                                                                                                         | Reference                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Step 1 | Create a fault-tolerant VLAN and identify peer IP addresses and configure peer appliances for heartbeat count and interval.                                  | <a href="#">Configuring High Availability Peers, page 11-8</a>                        |
| Step 2 | Create a fault-tolerant group, assign peer priorities, associate the group with a context, place the group in service, and enable automatic synchronization. | <a href="#">Configuring ACE High Availability Groups, page 11-11</a>                  |
| Step 3 | Configure tracking for switchover.                                                                                                                           | <a href="#">High Availability Tracking and Failure Detection Overview, page 11-17</a> |

## Related Topics

- [Understanding ACE Redundancy, page 11-2](#)
- [High Availability Polling, page 11-2](#)
- [Synchronizing High Availability Configurations with ACE Appliance Device Manager, page 11-6](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [High Availability Tracking and Failure Detection Overview, page 11-17](#)

# Configuring High Availability Peers



## Note

This functionality is available for only Admin contexts.

Fault-tolerant peers use a fault-tolerant VLAN to transmit and receive heartbeat packets and state and configuration replication packets. The standby member uses the heartbeat packet to monitor the health of the active member, while the active member uses the heartbeat packet to monitor the health of the standby member. When the heartbeat packets are not received from the active member when expected, switchover occurs and the standby member assumes all active communications previously on the active member.

Use this procedure to:

- Identify the two members of a high availability pair.
- Assign IP addresses to the peer ACE appliances.
- Assign a fault-tolerant VLAN to high availability peers and bind a physical Gigabit Ethernet interface to the FT VLAN.
- Configure heartbeat frequency and count on the ACE appliances in a fault-tolerant VLAN.

**Assumption**

- At least one fault-tolerant VLAN has been configured.



**Note** A fault-tolerant VLAN cannot be used for other network traffic.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management window appears with two columns: One for the selected ACE appliance and one for a peer ACE appliance.
- Step 2** Click **Edit**, and then enter the information for the primary appliance and the peer appliance as described in [Table 11-2](#).

**Table 11-2** ACE High Availability Management Configuration Attributes

| Field                 | This Appliance                                                                                                                                                                                                                             | Peer Appliance                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN                  | Specify a fault-tolerant VLAN to be used for this high availability pair. Valid entries are integers from 2 to 4094.<br><br><b>Note</b> This VLAN cannot be used for other network traffic.                                                | Not applicable.                                                                                                                                                                   |
| Interface             | Select the interface (specified by <i>slot_number/port_number</i> where <i>slot_number</i> is the physical slot on the ACE appliance, and <i>port_number</i> is the physical Ethernet data port on the ACE appliance) or the port channel. | Not applicable.                                                                                                                                                                   |
| IP Address            | Enter an IP address for the fault-tolerant VLAN in dotted-decimal format, such as 192.168.11.2.                                                                                                                                            | Enter the IP address of the peer interface in dotted-decimal format so that the peer appliance can communicate on the fault-tolerant VLAN.                                        |
| Netmask               | Select the subnet mask that is to be used for the fault-tolerant VLAN.                                                                                                                                                                     | Not applicable.                                                                                                                                                                   |
| Management IP Address | Enter the IP address for the ACE.                                                                                                                                                                                                          | Enter the Management IP Address of the peer appliance. When you enter this information, you can click on the HA Peer hyperlink in the <b>Config &gt; Virtual Contexts</b> screen. |
| Query VLAN            | Select the VLAN that the standby appliance is to use to determine whether the active appliance is down or if there is a connectivity problem with the fault-tolerant VLAN.                                                                 | Not applicable.                                                                                                                                                                   |

**Table 11-2** *ACE High Availability Management Configuration Attributes (continued)*

| Field                    | This Appliance                                                                                                                                                                                                                                   | Peer Appliance  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Heartbeat Count          | Enter the number of heartbeat intervals that must occur when no heartbeat packet is received by the standby appliance before the standby appliance determines that the active member is not available. Valid entries are integers from 10 to 50. | Not applicable. |
| Heartbeat Interval       | Enter the number of milliseconds that the active appliance is to wait between each heartbeat it sends to the standby appliance. Valid entries are integers from 100 to 1000.                                                                     | Not applicable. |
| Interface Enabled        | Check the Interface Enabled check box to enable the high availability interface. Clear the check box to disable the high availability interface.                                                                                                 | Not applicable. |
| Shared VLAN Host ID      | Enter a specific bank of MAC addresses that the ACE uses. Valid entries are integers from 1 to 16. Be sure to configure different bank numbers for multiple ACEs.                                                                                | Not applicable. |
| Peer Shared VLAN Host ID | Enter a specific bank of MAC addresses for the same ACE in a redundant configuration. Valid entries are integers from 1 to 16. Be sure to configure different bank numbers for multiple ACEs.                                                    | Not applicable. |
| HA State                 | This is a read-only field with the current state of high availability on the ACE appliance.                                                                                                                                                      | Not applicable. |

**Step 3** Do the following:

- Click **Deploy Now** to save your entries and to continue with configuring high availability groups. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom. See [Configuring ACE High Availability Groups, page 11-11](#) to configure a high availability group.
- Click **Cancel** to exit this procedure without saving your entries and to view the ACE HA Management screen.

**Related Topics**

- [Understanding ACE Redundancy, page 11-2](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)

## Clearing High Availability Pairs

**Note**

This functionality is available for only Admin contexts.

Use this procedure to remove a high availability link between two ACE appliances.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears.
- Step 2** Select the ACE appliance pair whose high availability configuration you want to remove, and then click **Clear**. A message appears asking you to confirm the clearing of the high availability link.
- Step 3** Do the following:
  - Click **OK** to confirm the removal of this high availability link and to return to the ACE HA Management screen.
  - Click **Cancel** to exit this procedure without removing this high availability link and to return to the ACE HA Management screen.

### Related Topics

- [Understanding ACE Redundancy, page 11-2](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Editing ACE High Availability Groups, page 11-14](#)
- [High Availability Tracking and Failure Detection Overview, page 11-17](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)
- [Tracking Hosts for High Availability, page 11-20](#)

## Configuring ACE High Availability Groups

**Note**

This functionality is available for only Admin contexts.

A fault-tolerant group consists of a maximum of two contexts: One active context on one appliance and one standby context on the peer appliance. You can create multiple fault-tolerant groups on each ACE appliance up to a maximum of 21 groups (20 user contexts and 1 Admin context).

Use this procedure to configure high availability groups.


**Note**

For the replication process to function properly and successfully replicate the configuration for a user context when switching from the active context to the standby context, ensure that each user context has been added to the FT group. All applicable user contexts must be part of an FT group for redundancy to function properly.

**Assumption**

At least one high availability pair has been configured. (See [Configuring High Availability Peers](#), page 11-8.)

**Procedure**

- 
- Step 1** **Config > Virtual Contexts > High Availability (HA) > Setup.** The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, click **Add** to add a new high availability group. The table refreshes with the configurable fields.
- Step 3** Check the Enabled check box to enable the high availability group. Clear the Enabled check box to disable the high availability group.
- Step 4** In the Context field, select the virtual context to associate with this high availability group.
- Step 5** In the Priority (Actual) field, enter the priority you want to assign to the first appliance in the group. Valid entries are integers from 1 to 255.
- A member of a fault-tolerant group becomes the active member through a process based on the priority assigned. In this process, the group member with the higher priority becomes the active member. When you set up a fault-tolerant pair, use a higher priority for the group where the active member initially resides.
- Step 6** Check the Preempt check box to indicate that the group member with the higher priority is to always assert itself and become the active member. Clear the Preempt check box to indicate that you do not want the group member with the higher priority to always become the active member.
- Step 7** In the Peer Priority (Actual) field, enter the priority you want to assign to the peer appliance in the group. Valid entries are integers from 1 to 255.
- A member of a fault-tolerant group becomes the active member through a process based on the priority assigned. In this process, the group member with the higher priority becomes the active member. When you set up a fault-tolerant pair, use a higher priority for the group where the active member initially resides.
- Step 8** Check the Autosync Run check box to enable automatic synchronization of the running configuration files. Clear the Autosync Run check box to disable automatic synchronization of the running configuration files. If you disable automatic synchronization, you need to update the configuration of the standby context manually.
- 

**Note** To understand how synchronization works between the active and the standby ACE appliances, see [Understanding ACE Redundancy](#), page 11-2 and [Redundancy Configuration Requirements and Restrictions](#), page 11-6.
- 
- Step 9** Check the Autosync Startup check box to enable automatic synchronization of the startup configuration files. Clear the Autosync Run check box to disable automatic synchronization of the startup configuration files. If you disable automatic synchronization, you need to update the configuration of the standby context manually. See [Manually Synchronizing Individual Virtual Context Configurations](#), page 4-82.
- Step 10** Do the following:
- Click **Deploy Now** to accept your entries. The ACE HA Groups table refreshes with the new high availability group.



- Click **Cancel** to exit this procedure without saving your entries and to return to the ACE HA Management screen and ACE HA Groups table.

**Step 11** (Optional) To display statistics and status information for a particular high availability group, choose the group from the ACE HA Groups table, and click **Details**.

The **show ft group *group\_id* detail** CLI command output appears. See the “[Displaying High Availability Group Statistics and Status Information](#)” section on page 11-16 for details.

---

#### Related Topics

- [Configuring High Availability Peers, page 11-8](#)
- [Editing ACE High Availability Groups, page 11-14](#)
- [High Availability and Virtual Context Configuration Status, page 4-81](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)
- [Tracking Hosts for High Availability, page 11-20](#)

## Editing ACE High Availability Groups

**Note**

This functionality is available for only Admin contexts.

Use this procedure to modify the attributes of a high availability group.

**Note**

If you need to modify a fault-tolerant group, take the group out of service before making any other changes (see [Taking a High Availability Group Out of Service, page 11-15](#)). When you finish making all changes, place the group back into service (see [Enabling a High Availability Group, page 11-15](#)).

### Procedure

- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group you want to modify, and then click **Edit**. The table refreshes with configurable fields.
- Step 3** Modify the fields as desired. For information on these fields, see [Configuring ACE High Availability Groups, page 11-11](#).
- Step 4** When you finish modifying this group, do the following:
  - Click **Deploy Now** to accept your entries and to return to the ACE HA Groups table.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the ACE HA Management screen.

### Related Topics

- [Taking a High Availability Group Out of Service, page 11-15](#)
- [Enabling a High Availability Group, page 11-15](#)
- [Configuring High Availability Peers, page 11-8](#)
- [High Availability Tracking and Failure Detection Overview, page 11-17](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)
- [Tracking Hosts for High Availability, page 11-20](#)

## Taking a High Availability Group Out of Service

**Note**

This functionality is available for only Admin contexts.

If you need to modify a fault-tolerant group, you must first take the group out of service before making any other changes. Use this procedure to take a high availability group out of service.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group you want to take out of service, and then click **Edit**. The table refreshes with configurable fields.
- Step 3** Clear the **Enabled** check box.
- Step 4** Click **Deploy Now** to take the high availability group out of service and to return to the ACE HA Groups table.

You can now make the necessary modifications to the high availability group. To put the high availability group back in service, see [Enabling a High Availability Group, page 11-15](#).

**Related Topic**

- [Enabling a High Availability Group, page 11-15](#)

## Enabling a High Availability Group

**Note**

This functionality is available for only Admin contexts.

After you take a high availability group out of service to modify it, you need to reenable the group. Use the following procedure to put a high availability group back in service.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group you want to take out of service, and then click **Edit**. The table refreshes with configurable fields.
- Step 3** Check the **Enabled** check box.
- Step 4** Click **Deploy Now** to put the high availability group in service and to return to the ACE HA Groups table.

**Related Topic**

- [Taking a High Availability Group Out of Service, page 11-15](#)

## Displaying High Availability Group Statistics and Status Information

You can display statistics and status information for a particular high availability group by using the **Details** button. DM accesses the **show ft group group\_id detail** CLI command to display detailed ACE HA group information.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**.  
The HA Management window appears at the top of the content area and the HA Groups table appears at the bottom.
- Step 2** Choose an ACE HA group from the ACE HA Groups table and click **Details**.  
The **show ft group group\_id detail** CLI command output appears. For details on the displayed output fields, see the *Administration Guide, Cisco ACE Application Control Engine*.
- Step 3** Click **Update Details** to refresh the output for the **show ft group group\_id detail** CLI command.
- Step 4** Click **Close** to return to the VLAN Interfaces table.
- 

### Related Topics

- [Understanding ACE Redundancy, page 11-2](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)

## Switching Over a High Availability Group



### Note

This functionality is available for only Admin contexts.

You may need to cause a switchover when you want to make a particular context the standby (for example, for maintenance or a software upgrade on the currently active context). If the standby group member can statefully become the active member of the high availability group, a switchover occurs.

Use this procedure to force the failover of a high availability group.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the group you want to switch over, and then click **Switchover**. The standby group member becomes active, while the previously active group member becomes the standby member.
-

**Related Topics**

- [Understanding ACE Redundancy, page 11-2](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)

## Deleting ACE High Availability Groups

**Note**

This functionality is available for only Admin contexts.

Use this procedure to remove a high availability group from ACE Appliance Device Manager management.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group that you want to remove, and then click **Delete**. A message appears asking you to confirm the deletion.
- Step 3** Do the following:
- Click **Deploy Now** to delete the high availability group and to return to the ACE HA Groups table. The selected group no longer appears.
  - Click **Cancel** to exit this procedure without deleting the high availability group and to return to the ACE HA Groups table.
- 

**Related Topics**

- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)

## High Availability Tracking and Failure Detection Overview

The tracking and detection of failures ensures that switchover occurs as soon as the criteria are met (see [Configuring High Availability Peers, page 11-8](#)). With the ACE Appliance Device Manager, you can track and detect failures on:

- Hosts—See [Tracking Hosts for High Availability, page 11-20](#).
- Interfaces—See [Tracking VLAN Interfaces for High Availability, page 11-19](#).

When the active member of a fault-tolerant group becomes unresponsive, the following occurs:

1. The active member's priority is reduced by 10.

2. If the resulting priority value is less than that of the standby member, the active member switches over and the standby member becomes the new active member. All active flows continue uninterrupted.
3. When the failed member comes back up, its priority is incremented by 10.
4. If the resulting priority value is greater than that of the currently active member, a switchover occurs again, returning the flows to the originally active member.

**Note**

---

In a user context, the ACE appliance allows a switchover only of the fault-tolerant groups belonging to that context. In an Admin context, the ACE appliance allows a switchover of all fault-tolerant groups on all configured contexts on the appliance.

---

**Related Topics**

- [Configuring ACE High Availability Groups, page 11-11](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)
- [Tracking Hosts for High Availability, page 11-20](#)

# Tracking VLAN Interfaces for High Availability

Use this procedure to configure a tracking and failure detection process for a VLAN interface.

**Note**

When a virtual context is in either the Standby Hot or Standby Warm state (see [High Availability Polling, page 11-2](#)), the virtual context may receive configuration changes from its ACE peer without updating the Device Manager GUI. As a result, the ACE appliance Device Manager GUI will be out of synchronization with the CLI configuration. If you need to check configuration on a standby virtual context using the tracking and failure detection process, we recommend that you first perform a manual synchronization using either the CLI Sync or CLI Sync All buttons before checking the configuration values.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > HA Tracking And Failure Detection > Interfaces**. The Track Interface table appears.
- Step 2** Click **Add** to add a new tracking process to this table, or select an existing entry, and then click **Edit** to modify it. The Track Interface configuration screen appears.
- Step 3** In the Track Object Name field, enter a unique identifier for the tracking process. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 4** In the Priority field, enter the priority for the interface on the active member. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. The values that you enter here and in the Interface Peer Priority field (see [Step 6](#)) reflect the point at which you want switchover to occur. If the tracked interface goes down, the priority of that fault-tolerant group is decremented by the value entered in the Priority field. If the priority of the fault-tolerant group on the active member falls below that of the standby member, a switchover occurs.
- Step 5** In the VLAN Interface field, select the fault-tolerant VLAN that you want the active member to track.
- Step 6** In the Interface Peer Priority field, enter the priority for the interface on the standby member. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. The values that you enter here and in the Priority field (See [Step 4](#)) reflect the point at which you want switchover to occur. If the tracked interface goes down, the priority of that fault-tolerant group is decremented by the value entered in the Interface Peer Priority field. If the priority of the fault-tolerant group on the active member falls below that of the standby member, a switchover occurs.
- Step 7** In the Peer VLAN Interface field, enter the identifier of an existing fault-tolerant VLAN that you want the standby member to track. Valid entries are integers from 1 to 4096.
- Step 8** Do the following:
  - Click **Deploy Now** to save your entries and to return to the Track Interface table.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Track Interface table.
  - Click **Next** to save your entries and to configure the next entry in the Track Interface table.

**Related Topics**

- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)

- [Tracking Hosts for High Availability, page 11-20](#)

## Tracking Hosts for High Availability

Use this procedure to configure a tracking and failure detection process for a gateway or host.

### Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; HA Tracking And Failure Detection &gt; Hosts</b> . The Track Host table appears.                                                                                                                                                                                                                                                                                                                               |
| <b>Step 2</b> | Click <b>Add</b> to add a new tracking process to the table, or select an existing entry, and then click <b>Edit</b> to modify it. The Track Host configuration screen appears.                                                                                                                                                                                                                                                                            |
| <b>Step 3</b> | In the Track Object Name field, enter a unique identifier for the tracking process. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                    |
| <b>Step 4</b> | For the IP Address Type, select either IPv4 or IPv6 for the host address type.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 5</b> | In the Track Host/IP Address field, enter the IPv4 or IPv6 address or hostname of the gateway or host that you want the active member of the high availability group to track.                                                                                                                                                                                                                                                                             |
| <b>Step 6</b> | In the Priority field, enter the priority of the probe sent by the active member. Valid entries are integers from 0 to 255. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the host that the probe is tracking. If the probe goes down, the ACE appliance decrements the priority of the fault-tolerant group on the active member by the value in the Priority field.                              |
| <b>Step 7</b> | In the Peer Host/IP Address field, enter the IPv4 or IPv6 address or hostname of the host that you want the standby member to track.                                                                                                                                                                                                                                                                                                                       |
| <b>Step 8</b> | In the Peer Priority field, enter the priority of the probe sent by the standby member. Valid entries are integers from 0 to 255. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the host that the probe is tracking. If the probe goes down, the ACE appliance decrements the priority of the fault-tolerant group on the standby member by the value in the Priority field.                       |
| <b>Step 9</b> | Do the following: <ul style="list-style-type: none"><li>• Click <b>Deploy Now</b> to save your entries and to continue with configuring track host probes. See <a href="#">Configuring Host Tracking Probes, page 11-21</a>.</li><li>• Click <b>Cancel</b> to exit this procedure without saving your entries and to return to the Track Host table.</li><li>• Click <b>Next</b> to save your entries and to configure another tracking process.</li></ul> |
- 

### Related Topics

- [Configuring Host Tracking Probes, page 11-21](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)



# Configuring Host Tracking Probes

Use this procedure to configure probes on the active high availability group member to track the health of the gateway or host.

## Assumptions

- At least one host tracking process for high availability has been configured (see [Tracking Hosts for High Availability](#), page 11-20.)
- At least one health monitoring probe has been configured (see [Configuring Health Monitoring for Real Servers](#), page 6-41).

## Procedure

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; HA Tracking And Failure Detection &gt; Hosts</b> . The Track Host table appears.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 2</b> | Select the tracking process you want to configure a probe for, and then select the <b>Track Host Probe</b> tab. The Track Host Probe table appears.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 3</b> | In the Track Host Probe table, click <b>Add</b> to add a track host probe, or select an existing track host probe, and then click <b>Edit</b> to modify it. The Track Host Probe configuration screen appears.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 4</b> | In the Probe Name field, select the name of the probe to be used for the host tracking process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 5</b> | In the Priority field, enter a priority for the host you are tracking by the active member of the high availability group. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. Assign a priority value based on the relative importance of the gateway or host that the probes are tracking. If the host goes down, the ACE appliance decrements the priority of the high availability group on the active member by the value in this Priority field. If the resulting priority of the high availability group on the active member is less than the priority of the high availability group on the standby member, a switchover occurs. |
| <b>Step 6</b> | Do the following: <ul style="list-style-type: none"><li>• Click <b>Deploy Now</b> to save your entries and to return to the Track Host Probe table. The table includes the added probe.</li><li>• Click <b>Cancel</b> to exit this procedure without saving your entries and to return to the Track Host Probe table.</li><li>• Click <b>Next</b> to save your entries and to configure another track host probe.</li></ul>                                                                                                                                                                                                                                                     |
- 

## Related Topics

- [Configuring Peer Host Tracking Probes](#), page 11-22
- [Configuring High Availability Peers](#), page 11-8
- [Configuring ACE High Availability Groups](#), page 11-11
- [Tracking VLAN Interfaces for High Availability](#), page 11-19

## Deleting Host Tracking Probes

Use this procedure to remove a high availability host tracking probe.

### Procedure

- 
- |               |                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; HA Tracking And Failure Detection &gt; Hosts</b> . The Track Host table appears.                                                          |
| <b>Step 2</b> | Select the tracking process you want to modify, and then select the Track Host Probe tab. The Track Host Probe table appears.                                                         |
| <b>Step 3</b> | In the Track Host table, select the probe you want to remove, and then click <b>Delete</b> . The probe is deleted and the Track Host Probe table refreshes without the deleted probe. |
- 

### Related Topics

- [Configuring Peer Host Tracking Probes, page 11-22](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)

## Configuring Peer Host Tracking Probes

Use this procedure to configure probes on the standby member of a high availability group to track the health of the gateway or host.

### Assumptions

- At least one host tracking process for high availability has been configured (see [Tracking Hosts for High Availability, page 11-20](#).)
- At least one health monitoring probe has been configured (see [Configuring Health Monitoring for Real Servers, page 6-41](#)).

### Procedure

- 
- |               |                                                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; HA Tracking And Failure Detection &gt; Hosts</b> . The Track Host table appears.                                                                                                               |
| <b>Step 2</b> | Select the tracking process you want to modify, and then select the Peer Track Host Probe tab. The Peer Track Host Probes table appears.                                                                                                   |
| <b>Step 3</b> | In the Peer Track Host Probes table, click <b>Add</b> to add a peer host tracking probe, or select an existing peer host tracking probe, and then click <b>Edit</b> to modify it. The Peer Track Host Probes configuration screen appears. |
| <b>Step 4</b> | In the Probe Name field, select the name of the probe to be used for the peer host tracking process.                                                                                                                                       |

- Step 5** In the Priority field, enter a priority for the host you are tracking by the standby member of the high availability group. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. Assign a priority value based on the relative importance of the gateway or host that the probes are tracking. If the host goes down, the ACE appliance decrements the priority of the high availability group on the standby member by the value in this Priority field.
- Step 6** Do the following:
- Click **Deploy Now** to save your entries and to return to the Peer Track Host Probes table. The table includes the added probe.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Peer Track Host Probes table.
  - Click **Next** to save your entries and to configure another peer track host probe.
- 

**Related Topics**

- [Configuring Host Tracking Probes, page 11-21](#)
- [Configuring High Availability Peers, page 11-8](#)
- [Configuring ACE High Availability Groups, page 11-11](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)

## Deleting Peer Host Tracking Probes

Use this procedure to remove a high availability peer host tracking probe.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > HA Tracking And Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to modify then, select the Peer Track Host Probe tab. The Peer Track Host Probes table appears.
- Step 3** In the Peer Track Host Probes table, select the probe you want to remove, and then click **Delete**. The probe is deleted and the Peer Track Host Probes table refreshes without the deleted probe.
- 

**Related Topics**

- [Configuring Peer Host Tracking Probes, page 11-22](#)
- [Configuring Host Tracking Probes, page 11-21](#)
- [Tracking VLAN Interfaces for High Availability, page 11-19](#)





# CHAPTER 12

## Configuring Traffic Policies

---

This chapter describes how to configure traffic policies. ACE Appliance Device Manager helps you configure class maps and policy maps to provide a global level of classification for filtering traffic received by or passing through the ACE appliance. You create traffic policies and attach these policies to one or more VLAN interfaces associated with the ACE appliance to apply feature-specific actions to the matching traffic. The ACE appliance uses the individual traffic policies to implement functions such as:

- Remote access using Secure Shell (SSH) or Telnet
- Server load balancing
- Network Address Translation (NAT)
- Optimization of HTTP traffic
- HTTP deep packet inspection, application protocol inspection, FTP command inspection, Skinny Client Control Protocol (SCCP) deep packet inspection, or SIP inspection
- Secure Socket Layer (SSL) security services between a Web browser (the client) and the HTTP connection (the server)
- TCP termination, normalization, and reuse
- IP normalization and fragment reassembly



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

### Related Topics

- [Class Map and Policy Map Overview, page 12-2](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Setting Match Conditions for Class Maps, page 12-10](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)
- [Configuring Actions Lists, page 12-90](#)

# Class Map and Policy Map Overview

You classify inbound network traffic destined to, or passing through, the ACE appliance based on a series of flow match criteria specified by a class map. Each class map defines a traffic classification; that is, network traffic that is of interest to you. A policy map defines a series of actions (functions) that you want applied to a set of classified inbound traffic.

Class maps enable you to classify network traffic based on the following criteria:

- Layer 3 and Layer 4 traffic flow information—Source or destination IP address, source or destination port, virtual IP address, IP protocol and port, or management protocol
- Layer 7 protocol information—HTTP cookie, HTTP URL, HTTP header, HTTP content, FTP request commands, RADIUS, RDP, RTSP, Skinny, or SIP

Table 12-1 lists the available policies for the ACE.

**Table 12-1** Traffic Policies

| Policy Map                                               | Description                                                                       |
|----------------------------------------------------------|-----------------------------------------------------------------------------------|
| Layer 3/4 Management Traffic (First-Match)               | Layer 3 and Layer 4 policy map for network management traffic received by the ACE |
| Layer 3/4 Network Traffic (First-Match)                  | Layer 3 and Layer 4 policy map for traffic passing through the ACE                |
| Layer 7 Command Inspection - FTP (First-Match)           | Layer 7 policy map for inspection of FTP commands                                 |
| Layer 7 Deep Packet Inspection - HTTP (All-Match)        | Layer 7 policy map for inspection of HTTP packets                                 |
| Layer 7 Deep Packet Inspection - SIP (All-Match)         | Layer 7 policy map for inspection of SIP packets                                  |
| Layer 7 Deep Packet Inspection - Skinny                  | Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)        |
| Layer 7 HTTP Optimization (First-Match)                  | Layer 7 policy map for optimizing HTTP traffic                                    |
| Layer 7 Server Load Balancing (First-Match)              | Layer 7 policy map for HTTP server load balancing                                 |
| Server Load Balancing - Generic (First-Match)            | Generic Layer 7 policy map for server load balancing                              |
| Server Load Balancing - HTTPS <sup>1</sup> (First-Match) | Layer 7 policy map for HTTPS server load balancing                                |
| Server Load Balancing - RADIUS (First-Match)             | Layer 7 policy map for RADIUS server load balancing                               |
| Server Load Balancing - RDP (First-Match)                | Layer 7 policy map for RDP server load balancing                                  |
| Server Load Balancing - RTSP (First-Match)               | Layer 7 policy map for RTSP server load balancing                                 |

1. This option is not available for ACE NPE software image.

The traffic classification process consists of the following three steps:

1. Creating a class map, which comprise a set of match criteria related to Layer 3 and Layer 4 traffic classifications or Layer 7 protocol classifications.

2. Creating a policy map, which refers to the class maps and identifies a series of actions to perform based on the traffic match criteria.
3. Activating the policy map and attaching it to a specific VLAN interface or globally to all VLAN interfaces associated with a context by configuring a virtual context global traffic policy to filter traffic received by the ACE appliance.

The following overview topics describe the components that define a traffic policy:

- [Class Maps, page 12-3](#)
- [Policy Maps, page 12-4](#)
- [Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5](#)
- [Application Protocol Inspection Overview, page 12-5](#)
- [Configuring Virtual Context Global Traffic Policies, page 4-28](#)

## Class Maps

A class map defines each type of Layer 3 and Layer 4 traffic class and each Layer 7 protocol class. You create class maps to classify the traffic received and transmitted by the ACE appliance.

- Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE appliance or network management traffic that can be received by the ACE appliance.
- Layer 7 protocol-specific classes identify server load balancing based on HTTP traffic, deep inspection of HTTP traffic, or the inspection of FTP commands by the ACE appliance.

A traffic class contains the following components:

- Class map name
- Class map type
- One or more match conditions that define the match criteria for the class map
- Instructions on how the ACE appliance evaluates match conditions when you specify more than one match statement in a traffic class (match-any, match-all)

The ACE supports a system-wide maximum of 8192 class maps.

The individual match conditions specify the criteria for classifying Layer 3 and Layer 4 network traffic as well as the Layer 7 HTTP server load balancing and application protocol-specific fields. The ACE appliance evaluates the packets to determine whether they match the specified criteria. If a statement matches, the ACE appliance considers that packet to be a member of the class and forwards the packet according to the specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class if one is specified.

The ACE appliance allows you to configure two Layer 7 HTTP load-balancing class maps in a nested traffic class configuration to create a single traffic class. You can perform Layer 7 class map nesting to achieve complex logical expressions. The ACE appliance restricts the nesting of class maps to two levels to prevent you from including one nested class map under a different class map.

### Related Topics

- [Class Map and Policy Map Overview, page 12-2](#)
- [Policy Maps, page 12-4](#)
- [Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5](#)

- [Application Protocol Inspection Overview, page 12-5](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)

## Policy Maps

A policy map creates the traffic policy. The purpose of a traffic policy is to implement specific ACE appliance functions associated with a traffic class. A traffic policy contains the following components:

- Policy map name
- Previously created traffic class map or, optionally, the default class map
- One or more of the individual Layer 3 and Layer 4 or Layer 7 policies that specify the actions to be performed by the ACE appliance

The ACE appliance supports a system-wide maximum of 4096 policy maps.

A Layer 7 policy map is always associated within a Layer 3 and Layer 4 policy map to provide an entry point for traffic classification. Layer 7 policy maps are considered to be child policies and can only be nested under a Layer 3 and Layer 4 policy map. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface; a Layer 7 policy map cannot be directly applied on an interface. For example, to associate a Layer 7 load-balancing policy map, you nest the load-balancing policy map by using the Layer 3 and Layer 4 Policy map action type.

If none of the classifications specified in policy maps match, then the ACE appliance executes the default actions specified against the class map configured with the Use Class Default option to use a default class map (if specified). All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. The Use Class Default feature has an implicit match-any match statement and is used to match any traffic classification.

The ACE appliance supports flexible class map ordering within a policy map. The ACE appliance executes only the actions for the first matching traffic classification, so the order of class maps within a policy map is very important. The policy lookup order is based on the security features of the ACE appliance. The policy lookup order is implicit, irrespective of the order in which you configure policies on the interface.

The policy lookup order of the ACE appliance is as follows:

1. Access control (permit or deny a packet)
2. Permit or deny management traffic
3. TCP/UDP connection parameters
4. Load balancing based on a virtual IP (VIP)
5. Application protocol inspection
6. Source NAT
7. Destination NAT

The sequence in which the ACE appliance applies the actions for a specific policy is independent of the actions configured for a class map inside a policy.

### Related Topics

- [Class Map and Policy Map Overview, page 12-2](#)
- [Policy Maps, page 12-4](#)



- [Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5](#)
- [Application Protocol Inspection Overview, page 12-5](#)
- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps

Parameter maps allow you to combine related actions in a Layer 3 and Layer 4 policy map. For example, an HTTP parameter map provides a means of performing actions on traffic received by the ACE appliance based on certain criteria such as HTTP header and cookie settings, server connection reuse, action to be taken when an HTTP header, cookie or URL exceeds a configured maximum length, and so on.

The ACE appliance uses policy maps to combine class maps and parameter maps into traffic policies and to perform certain configured actions on the traffic that matches the specified criteria in the policies.

See [Table 8-1](#) for a list of available ACE appliance parameter maps.

### Related Topics

- [Configuring Parameter Maps, page 8-1](#)
- [Class Map and Policy Map Overview, page 12-2](#)
- [Class Maps, page 12-3](#)
- [Policy Maps, page 12-4](#)
- [Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 12-5](#)
- [Application Protocol Inspection Overview, page 12-5](#)

## Application Protocol Inspection Overview

Certain applications require special handling of the data portion of a packet as the packets pass through the ACE. Application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic passing through the ACE. Based on the specifications of the traffic policy, the ACE accepts or rejects the packets to ensure the secure use of applications and services.

Certain applications require special handling of the data portion of a packet as the packets pass through the ACE appliance. Application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic passing through the ACE appliance. Based on the specifications of the traffic policy, the ACE appliance accepts or rejects the packets to ensure the secure use of applications and services.

You can configure the ACE to perform application protocol inspection, sometimes referred to as an application protocol “fixup” for applications that do the following:

- Embed IP addressing information in the data packet including the data payload.
- Open secondary channels on dynamically assigned ports.

You may require the ACE to perform application inspection of Domain Name System (DNS), FTP (File Transfer Protocol), H.323, HTTP, Internet Control Message Protocol (ICMP), Internet Locator Service (ILS), Real-Time Streaming Protocol (RTSP), Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP) as a first step before passing the packets to the destination server. For HTTP, the ACE performs deep packet inspection to statefully monitor the HTTP protocol and permit or deny

traffic based on user-defined traffic policies. HTTP deep packet inspection focuses mainly on HTTP attributes such as the HTTP header, the URL, and the payload. For FTP, the ACE performs FTP command inspection for FTP sessions, allowing you to restrict specific commands by the ACE.

Application inspection helps you to identify the location of the embedded IP addressing information in the TCP or UDP flow. This inspection allows the ACE to translate embedded IP addresses and to update any checksum or other fields that are affected by the translation.

Translating IP addresses embedded in the payload of protocols is especially important for NAT (explicitly configured by the user) and server load balancing (an implicit NAT).

Application inspection also monitors TCP or UDP sessions to determine the port numbers for secondary channels. Some protocols open secondary TCP or UDP ports to improve performance. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application protocol inspection function monitors these sessions, identifies the dynamic port assignments, and permits data exchange on these ports for the duration of the session.

Table 12-2 describes the application inspection protocols supported by the ACE, the default TCP or UDP protocol and port, and whether the protocol is compatible with Network Address Translation (NAT) and Port Address Translation (PAT).

**Table 12-2**      *Application Inspection Support*

| Application Protocol | Transport Protocol | Port                | NAT/PAT Support | Enabled by Default | Standards <sup>1</sup> | Comments/Limitations                                                                                                                                                                                 |
|----------------------|--------------------|---------------------|-----------------|--------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DNS                  | UDP                | Src—Any<br>Dest—53  | NAT             | No                 | RFC 1123               | Inspects DNS packets destined to port 53. You can specify the maximum length of the DNS packet to be inspected.                                                                                      |
| FTP                  | TCP                | Src—Any<br>Dest—21  | Both            | No                 | RFC 959                | Inspects FTP packets, translates address and port embedded in the payload, and opens up a secondary channel for data.                                                                                |
| FTP strict           | TCP                | Src—Any<br>Dest—21  | Both            | No                 | RFC 959                | The FTP Strict field allows the ACE appliance to track each FTP command and response sequence, and also prevents an FTP client from determining valid usernames that are supported on an FTP server. |
| HTTP                 | TCP                | Src—Any<br>Dest—80  | Both            | No                 | RFC 2616               | Inspects HTTP packets.                                                                                                                                                                               |
| ICMP                 | ICMP               | Src—N/A<br>Dest—N/A | Both            | No                 | —                      | Allows ICMP traffic to have a “session” so that it can be inspected similarly to TCP and UDP traffic.                                                                                                |

Table 12-2 Application Inspection Support (continued)

| Application Protocol | Transport Protocol | Port                 | NAT/PAT Support | Enabled by Default | Standards <sup>1</sup>                                      | Comments/Limitations                                                                                                                                                                                                                                                                                           |
|----------------------|--------------------|----------------------|-----------------|--------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICMP error           | ICMP               | Src—N/A<br>Dest—N/A  | NAT             | No                 | —                                                           | The ICMP Error field supports NAT of ICMP error messages. When you enable ICMP error inspection, the ACE appliance creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The ACE appliance overwrites the packet with the translated IP addresses. |
| ILS                  | TCP                | Src—Any<br>Dest—389  | NAT             | No                 | RFC 2251 (LDAPv3)<br>Includes support for RFC 1777 (LDAPv2) | Referral requests and responses are not supported.<br>Users in multiple directories are not unified.<br>Single users having multiple identities in multiple directories cannot be recognized by NAT.                                                                                                           |
| RTSP                 | TCP                | Src—Any<br>Dest—554  | NAT             | No                 | RFC 2326, RFC 2327, RFC 1889                                | Inspects RTSP packets and translates the payload according to NAT rules. The ACE opens up the secondary channels for audio and video. Not all the RTSP methods (packet types) specified in the RFC are supported.                                                                                              |
| SCCP                 | TCP                | Src—Any<br>Dest—2000 | NAT             | No                 | —                                                           | The ACE does not support PAT with SCCP.                                                                                                                                                                                                                                                                        |
| SIP                  | TCP and UDP        | Src—Any<br>Dest—5060 | NAT             | No                 | RFC 2543, RFC 3261, RFC 3265, RFC 3428                      | The ACE does not support PAT with SIP.                                                                                                                                                                                                                                                                         |

1. The ACE is in compliance with these standards, but it does not enforce compliance on packets being inspected. For example, FTP commands are supposed to be in a particular order, but the ACE does not enforce the order.

For background information about application protocol inspection as performed by the ACE appliance, see the *Security Guide, Cisco ACE Application Control Engine*.

**Related Topics**

- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Setting Match Conditions for Class Maps, page 12-10](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Configuring Virtual Context Class Maps

Class maps are used to define each Layer 3 and Layer 4 traffic class and each Layer 7 protocol class. You create class maps to classify the traffic received and transmitted by the ACE appliance.

- Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE appliance or network management traffic that can be received by the ACE appliance.
- Layer 7 protocol-specific classes identify:
  - Server load balancing, based on generic, HTTP, RADIUS, RTSP, or SIP traffic
  - HTTP or SIP traffic for deep inspection
  - FTP traffic for inspection of commands

A traffic class contains:

- A class map name
- One or more match commands that define the match criteria for the class map
- Instructions on how the ACE appliance evaluates match commands when there is more than one match command in a traffic class

**Note**

To successfully delete a class map from a context, the class map must no longer be in use. To delete multiple class maps, none of the class maps must be in use. If you attempt to delete multiple class maps and one of the class maps is still in use, none of the class maps are deleted and a message appears stating that one of the class maps is in use. Remove the class map that is still in use from your selection, and then click **Delete**. The selected class maps are removed.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** Click **Add** to add a new class map, or select an existing class map, and then click **Edit** to modify it.
- Step 3** The Name field contains an automatically incremented number for the class map. You can leave the number as it is or enter a different, unique number.
- Step 4** In the Class Map Type field, select the type of class map you are creating ([Table 12-3](#)).

**Table 12-3**      *Class Maps Types*

| <b>Class Map</b>                      | <b>Related Topic</b>                                                                                    |
|---------------------------------------|---------------------------------------------------------------------------------------------------------|
| Layer 3/4 Management Traffic          | <a href="#">Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14</a>  |
| Layer 3/4 Network Traffic             | <a href="#">Setting Match Conditions for Class Maps, page 12-10</a>                                     |
| Layer 7 Command Inspection - FTP      | <a href="#">Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 12-30</a>      |
| Layer 7 Deep Packet Inspection - HTTP | <a href="#">Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps, page 12-25</a> |
| Layer 7 Deep Packet Inspection - SIP  | <a href="#">Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps, page 12-31</a>  |
| Layer 7 Server Load Balancing         | <a href="#">Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16</a>       |
| Server Load Balancing - Generic       | <a href="#">Setting Match Conditions for Generic Server Load Balancing Class Maps, page 12-19</a>       |
| Server Load Balancing - RADIUS        | <a href="#">Setting Match Conditions for RADIUS Server Load Balancing Class Maps, page 12-20</a>        |
| Server Load Balancing - RTSP          | <a href="#">Setting Match Conditions for RTSP Server Load Balancing Class Maps, page 12-21</a>          |
| Server Load Balancing - SIP           | <a href="#">Setting Match Conditions for SIP Server Load Balancing Class Maps, page 12-23</a>           |

**Step 5** For all selections except Layer 7 Command Inspection - FTP, in the Match Type field, select the method the ACE appliance is to use to evaluate multiple match statements when multiple match conditions exist in the class map:

- **Match-any**—Indicates that the class map is a match if at least one of the match conditions listed in the class map is satisfied.
- **Match-all**—Indicates that the class map is a match only if all match conditions listed in the class map are satisfied.

**Step 6** In the Description field, enter a brief description for this class map.

**Step 7** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to configure match conditions for this class map. See [Setting Match Conditions for Class Maps, page 12-10](#) for more information.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Class Maps table.
- Click **Next** to save your entries and to configure another class map.

#### **Related Topics**

- [Configuring Virtual Contexts, page 4-1](#)
- [Deleting Class Maps, page 12-10](#)
- [Setting Match Conditions for Class Maps, page 12-10](#)

- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Deleting Class Maps

To successfully delete a class map from a context, the class map must no longer be in use. To delete multiple class maps, none of the class maps must be in use.

### Assumption

The class map to be deleted is not being used.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** Select the class maps you want to delete, and then click **Delete**.

If you attempt to delete multiple class maps and one of the class maps is still in use, none of the class maps are deleted and a message appears stating that one of the class map is in use. Remove the class map that is still in use from your selection, and then click **Delete**. The Class Maps table refreshes and the deleted class maps no longer appear.

---

### Related Topics

- [Class Map and Policy Map Overview, page 12-2](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)

## Setting Match Conditions for Class Maps

[Table 12-4](#) lists the class maps available for the ACE and provides links to topics for setting match conditions:

**Table 12-4** *Class Maps and Match Conditions*

| Class Map                             | Related Topic                                                                                           |
|---------------------------------------|---------------------------------------------------------------------------------------------------------|
| Layer 3/4 Management Traffic          | <a href="#">Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14</a>  |
| Layer 3/4 Network Traffic             | <a href="#">Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 12-11</a>     |
| Layer 7 Command Inspection - FTP      | <a href="#">Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 12-30</a>      |
| Layer 7 Deep Packet Inspection - HTTP | <a href="#">Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps, page 12-25</a> |
| Layer 7 Deep Packet Inspection - SIP  | <a href="#">Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps, page 12-31</a>  |
| Layer 7 Server Load Balancing         | <a href="#">Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16</a>       |

*Table 12-4 Class Maps and Match Conditions (continued)*

| Class Map                       | Related Topic                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------|
| Server Load Balancing - Generic | <a href="#">Setting Match Conditions for Generic Server Load Balancing Class Maps, page 12-19</a> |
| Server Load Balancing - RADIUS  | <a href="#">Setting Match Conditions for RADIUS Server Load Balancing Class Maps, page 12-20</a>  |
| Server Load Balancing - RTSP    | <a href="#">Setting Match Conditions for RTSP Server Load Balancing Class Maps, page 12-21</a>    |
| Server Load Balancing - SIP     | <a href="#">Setting Match Conditions for SIP Server Load Balancing Class Maps, page 12-23</a>     |

## Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps

Use this procedure to specify the match criteria for a Layer 3/Layer 4 network traffic class map on the ACE appliance.

### Assumption

You have configured a Layer 3/Layer 4 class map and want to establish match conditions.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the Layer 3/4 network traffic class map you want to set match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the type of match condition to be used for this class map and configure any match-specific attributes as described in [Table 12-5](#).

*Table 12-5 Layer 3/Layer 4 Network Traffic Class Map Match Condition Attributes*

| Match Condition Type | Description                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access List          | Indicates that an access list is the match type for this match condition.<br>In the Extended ACL field, select the ACL to use as the match condition.                  |
| Any                  | Indicates that any Layer 3 or Layer 4 traffic passing through the ACE appliance meets the match condition.                                                             |
| Anyv6                | This option appears for Device Manager software Version A5(1.2) and later only. Any Layer 3 or Layer 4 IPv6 traffic passing through the ACE meets the match condition. |

Table 12-5 Layer 3/Layer 4 Network Traffic Class Map Match Condition Attributes (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination Address  | <p>Indicates that a destination address is the match type for this match condition.</p> <ol style="list-style-type: none"> <li>1. For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>2. In the Destination Address field, enter the destination IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>3. For an IPv4 destination address, in the Destination Netmask field, select the subnet mask of the IP address.<br/>For an IPv6 destination address, in the Destination Prefix-length field, enter the prefix length for the address.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Port                 | <p>Indicates that a UDP or TCP port or range of ports is the match type for this match condition.</p> <ol style="list-style-type: none"> <li>1. In the Port Protocol field, select TCP or UDP as the protocol to be matched.</li> <li>2. In the Port Operator field, select the match criteria for the port: <ul style="list-style-type: none"> <li>– Any—Indicates that any port using the selected protocol meets the match condition.</li> <li>– Equal To—Indicates that a specific port using the protocol meets the match condition.<br/>In the Port Number field, enter the port to be matched. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE appliance is to include all ports.</li> <li>– Range—Indicates that the port must be one of a range of ports to meet the match condition. <ol style="list-style-type: none"> <li>a. In the Lower Port Number field, enter the first port number in the port range for the match condition.</li> <li>b. In the Upper Port Number field, enter the last port number in the port range for the match condition.</li> </ol> Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE appliance is to include all ports.</li> </ul> </li> </ol> |
| Portv6               | <p>This option appears for Device Manager software Version A5(1.2) and later only. UDP or TCP port or range of ports for IPv6 traffic that is the match type for this match condition.</p> <p>For port configuration information, see <a href="#">Port</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



Table 12-5 Layer 3/Layer 4 Network Traffic Class Map Match Condition Attributes (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source Address       | <p>Indicates that a source IP address is the match type for this match condition.</p> <ol style="list-style-type: none"> <li>For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.<br/>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Virtual Address      | <p>Indicates that a virtual IP address is the match type for this match condition.</p> <ol style="list-style-type: none"> <li>For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>In the Virtual Address field, enter the virtual IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>For an IPv4 virtual address, in the Virtual Netmask field, select the subnet mask of the IP address.<br/>For an IPv6 virtual address, in the Virtual Prefix-length field, enter the prefix length for the address.</li> <li>In the Virtual Address Protocol field, select the protocol to be used for this match condition. For a list of protocols and their respective numbers, see <a href="#">Table 4-18</a>.<br/>Depending on the protocol that you select, additional fields appear. If they appear, enter the information described in the following steps.</li> <li>In the Port Operator field, select the match criteria for the port: <ul style="list-style-type: none"> <li>Any—Indicates that any port using the selected protocol meets the match condition.</li> <li>Equal To—Indicates that a specific port using the protocol meets the match condition.<br/>In the Port Number field, enter the port to be matched. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE appliance is to include all ports.</li> <li>Range—Indicates that the port must be one of a range of ports to meet the match condition. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE appliance is to include all ports. <ol style="list-style-type: none"> <li>In the Lower Port Number field, enter the first port number in the port range for the match condition.</li> <li>In the Upper Port Number field, enter the last port number in the port range for the match condition.</li> </ol> </li> </ul> </li> </ol> |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.



**Note** If you click **Deploy Now**, the ACE appliance drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to save your entries and to configure additional match conditions.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14](#)
- [Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)

## Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps

Use this procedure to identify the network management protocols that can be received by the ACE appliance.

#### Assumption

You have configured a network management class map and want to establish the match conditions.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the Layer 3/Layer 4 management class map you want to set match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match conditions you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** Enter the match conditions (see [Table 12-6](#)).

**Table 12-6**      *Management Class Map Match Conditions*

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sequence Number          | Enter an integer from 2 to 255 as the line number. The number entered here does not indicate a priority or sequence for the match conditions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Match Condition Type     | <p>Select <b>Management</b> to confirm that this is for Layer 3/Layer 4 management traffic.</p> <p><b>Note</b> To change the type of match condition, you must delete the class map and add it again with the correct match type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Management Protocol Type | <p>This field identifies the network management protocols that can be received by the ACE appliance.</p> <p>Select the allowed protocol for this match condition:</p> <ul style="list-style-type: none"> <li>• HTTP—Specifies the Hypertext Transfer Protocol (HTTP).</li> <li>• HTTPS—Specifies the Hypertext Transfer Protocol Secure (HTTPS) for connectivity with the ACE Appliance Device Manager GUI on the ACE appliance. Communication is performed using port 443.</li> <li>• ICMP—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping.</li> <li>• ICMPv6—Specifies the Internet Control Message Protocol version 6 (ICMPv6).</li> <li>• KALAP UDP—Specifies the KeepAlive Appliance Protocol over UDP.</li> <li>• SNMP—Specifies the Simple Network Management Protocol (SNMP).</li> <li>• SSH—Specifies a Secure Shell (SSH) connection to the ACE appliance.</li> <li>• TELNET—Specifies a Telnet connection to the ACE appliance.</li> <li>• XML-HTTPS—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS). Communication is performed using port 10443.</li> </ul> |
| Traffic Type             | <p>Select the type of traffic:</p> <ul style="list-style-type: none"> <li>• Any—Indicates that any client source IP address meets the match condition.</li> <li>• Source Address—Indicates that a specific source IP address is part of the match condition.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Source Address           | <p>This field appears if Source Address is selected for Traffic Type.</p> <p>Enter the source IP address of the client in dotted-decimal notation, such as 192.168.11.1.</p> <p>For ICMPv6, enter a complete IPv6 address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Source Netmask           | <p>This field appears if Source Address is selected for Traffic Type.</p> <p>Select the subnet mask for the source IP address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Source Prefix-length     | <p>This field appears if ICMPv6 is selected for the Management Protocol Type and Source Address is selected for Traffic Type.</p> <p>Enter the prefix length for the source IPv6 address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.



**Note** If you click **Deploy Now**, the ACE appliance drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to save your entries and to configure additional match conditions.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Server Farms, page 6-18](#)
- [Configuring Sticky Groups, page 7-11](#)

## Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps

Use this procedure to set match conditions for Layer 7 server load-balancing class maps.

#### Assumption

You have configured a load-balancing class map and want to establish the match conditions.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the Layer 7 server load balancing class map you want to set match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255 as the line number. The number entered here does not indicate a priority or sequence for the match conditions.
- Step 5** In the Match Condition Type field, select the type of match to use and configure condition-specific attributes as described in [Table 12-7](#).

Table 12-7 Layer 7 Server Load Balancing Class Map Match Conditions

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>A class map is to be used to establish a match condition.</p> <p>In the Class Map field, select the class map to apply to this match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| HTTP Content    | <p>Specific content contained within the HTTP entity-body is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| HTTP Cookie     | <p>An HTTP cookie is to be used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters.</li> <li>3. In the Secondary Cookie Matching check box, do one of the following: <ul style="list-style-type: none"> <li>– Clear the check box to indicate that the cookie being defined is a primary cookie.</li> <li>– Check the check box to indicate that the cookie being defined is a secondary cookie. You can specify the delimiters for cookies in a URL string by using an HTTP parameter map (see the <a href="#">“Configuring HTTP Parameter Maps”</a> section on page 8-2).</li> </ul> </li> </ol>                                                                                                                                                             |
| HTTP Header     | <p>An HTTP header is to be used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Header Name field, specify the header to match in one of the following ways: <ul style="list-style-type: none"> <li>– To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button, and then enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</li> <li>– To specify a standard HTTP header, click the second radio button, and then select an HTTP header from the list.</li> </ul> </li> <li>2. In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string in quotes. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol> |

Table 12-7 Layer 7 Server Load Balancing Class Map Match Conditions (continued)

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP URL        | <p>A portion of an HTTP URL is to be used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the URL Expression field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <i>www.hostname.domain</i>. For example, in the URL <i>www.anydomain.com/latest/whatsnew.html</i>, include only <i>/latest/whatsnew.html</i>.</li> <li>2. In the Method Expression field, enter the HTTP method to match. Valid entries are method names entered as unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. You can enter either one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).</li> </ol> |
| Source Address  | <p>The source IP address is to be used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>2. In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.<br/>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</li> </ol>                                                                                                                                                                                                                                                                                            |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.



**Note** If you click **Deploy Now**, the ACE appliance drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to save your entries and to configure additional match conditions.

**Related Topics**

- [Using Virtual Contexts, page 4-2](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Setting Match Conditions for Generic Server Load Balancing Class Maps

Use this procedure to set match conditions for a generic server load balancing class map.

### Assumption

You have configured a generic server load balancing class map and want to establish match criteria.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the generic server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 12-8](#).

**Table 12-8** Generic Server Load Balancing Class Map Match Conditions

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>A class map is used to establish a match condition.</p> <p>In the Class Map field, select the class map to use for this match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Layer 4 Payload | <p>Generic data parsing is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>In the Layer 4 Payload Regex field, enter the Layer 4 payload expression contained within the TCP or UDP entity body to use for this match condition. Valid entries are text strings with a maximum of 255 alphanumeric characters. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use for matching string expressions.</li> <li>In the Layer 4 Payload Offset field, enter the absolute offset where the Layer 4 payload expression search starts. The offset starts at the first byte of the TCP or UDP body. Valid entries are integers from 0 to 999.</li> </ol> |
| Source Address  | <p>A source IP address is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.</li> </ol> <p>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</p>                                                                                                                                      |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



**Note**

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to configure another match condition for this class map.

#### Related Topics

- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Setting Match Conditions for RADIUS Server Load Balancing Class Maps

Use this procedure to set match conditions for a RADIUS server load balancing class map.

#### Assumption

You have configured a RADIUS server load balancing class map and want to establish match criteria.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the RADIUS server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 12-9](#).



Table 12-9 RADIUS Server Load Balancing Class Map Match Conditions

| Match Condition    | Description                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Calling Station ID | A unique identifier of the calling station is used to establish a match condition.<br>In the RADIUS Calling Station ID field, enter the calling station identifier to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use for matching string expressions. |
| User Name          | A username is used to establish a match condition.<br>In the User Name field, enter the name to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use for matching string expressions.                                                                       |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



**Note** If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to configure another match condition for this class map.

#### Related Topics

- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Setting Match Conditions for RTSP Server Load Balancing Class Maps

Use this procedure to set match conditions for a RTSP server load balancing class map.

#### Assumption

You have configured a RTSP server load balancing class map and want to establish match criteria.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the RTSP server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255.

- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 12-10](#).

**Table 12-10** RTSP Server Load Balancing Class Map Match Conditions

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>A class map is used to establish a match condition.</p> <p>In the Class Map field, select the class map to use for this match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| RTSP Header     | <p>The name and value in an RTSP header are used to establish a match condition.</p> <ol style="list-style-type: none"> <li>In the Header Name field, specify the header in one of the following ways: <ul style="list-style-type: none"> <li>To specify an RTSP header that is not one of the standard RTSP headers, select the first radio button and enter the RTSP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</li> <li>To specify one of the standard RTSP headers, select the second radio button and select one of the RTSP headers from the list.</li> </ul> </li> <li>In the Header Value field, enter the header value expression string to compare against the value in the specified field in the RTSP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol> |
| RTSP URL        | <p>A URL or portion of a URL is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>In the URL Expression field, enter a URL, or portion of a URL, to match. The ACE performs matching on whatever URL string appears after the RTSP method, regardless of whether the URL includes the host name. The ACE supports regular expressions for matching URL strings. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> <li>In the Method Expression field, enter the RTSP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can be either one of the standard RTSP method names (DESCRIBE, ANNOUNCE, GET_PARAMETER, OPTIONS, PAUSE, PLAY, RECORD, REDIRECT, SETUP, SET_PARAMETER, TEARDOWN) or a text string that must be matched exactly (for example, STINGRAY).</li> </ol>                                                                                                                                                                                                                               |
| Source Address  | <p>The source IP address is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1.</li> <li>In the Source Netmask field, select the subnet mask for the source IP address.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



**Note** If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to configure another match condition for this class map.

#### Related Topics

- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Setting Match Conditions for SIP Server Load Balancing Class Maps

Use this procedure to set match conditions for a SIP server load balancing class map.

#### Assumption

You have configured a SIP server load balancing class map and want to establish match criteria.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the SIP server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 12-11](#).

Table 12-11 SIP Server Load Balancing Class Map Match Conditions

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>A class map is used to establish a match condition.</p> <p>In the Class Map field, select the class map to use for this match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SIP Header      | <p>A SIP header name and value are used to establish a match condition.</p> <ol style="list-style-type: none"> <li>In the Header Name field, specify the header in one of the following ways: <ul style="list-style-type: none"> <li>To specify a SIP header that is not one of the standard SIP headers, select the first radio button and enter the SIP header name in the Header Name field. Enter an unquoted text string with no spaces and a maximum of 64 characters.</li> <li>To specify one of the standard SIP headers, select the second radio button and select one of the SIP headers from the list.</li> </ul> </li> <li>In the Header Value field, enter the header value expression string to compare against the value in the specified field in the SIP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol> |
| Source Address  | <p>The source IP address is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.</li> </ol> <p>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.

**Note**

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to configure another match condition for this class map.

**Related Topics**

- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps

The ACE Appliance Device Manager allows you to create Layer 7 class maps and policy maps to be used for HTTP deep packet inspection by the ACE appliance. When these features are configured, the ACE appliance performs a stateful deep packet inspection of the HTTP protocol and permits or restricts traffic based on the actions in the defined policy maps. You can configure the following security features as part of HTTP deep packet inspection to be performed by ACE appliances:

- Regular expression matching on name in an HTTP header, URL name, or content expressions in an HTTP entity body
- Content, URL, and HTTP header length checks
- MIME-type message inspection
- Transfer-encoding methods
- Content type verification and filtering
- Port 80 misuse by tunneling protocols
- RFC compliance monitoring and RFC method filtering

Use this procedure to configure a Layer 7 class map for deep packet inspection of HTTP traffic.

### Assumption

You have configured a Layer 7 deep packet inspection class map and want to establish match conditions.

### Procedure

- 
- |               |                                                                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Class Maps</b> . The Class Maps table appears.                                                                                                                                     |
| <b>Step 2</b> | In the Class Maps table, select the Layer 7 HTTP deep packet inspection class map you want to set match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them. |
| <b>Step 3</b> | In the Match Condition table, click <b>Add</b> to add match criteria, or select the match condition you want to modify, and then click <b>Edit</b> . The Match Condition configuration screen appears.                                                  |
| <b>Step 4</b> | In the Sequence Number field, enter an integer from 2 to 255 as the line number. The number entered here does not indicate a priority or sequence for the match conditions.                                                                             |
| <b>Step 5</b> | In the Match Condition Type field, select the method by which match decisions are to be made and configure condition-specific attributes as described in <a href="#">Table 12-12</a> .                                                                  |

Table 12-12 HTTP Protocol Inspection Match Condition Types

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content              | <p>Specific content contained within the HTTP entity-body is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Content Length       | <p>The content parse length in an HTTP message is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Content Length Operator field, select the operand to be used to compare content length: <ul style="list-style-type: none"> <li>– Equal To—Indicates that the content length must equal the number in the Content Length Value (Bytes) field.</li> <li>– Greater Than—Indicates that the content length must be greater than the number in the Content Length Value (Bytes) field.</li> <li>– Less Than—Indicates that the content length must be less than the number in the Content Length Value (Bytes) field.</li> <li>– Range—Indicates that the content length must be within the range specified in the Content Length Lower Value (Bytes) field and the Content Length Higher Value (Bytes) field.</li> </ul> </li> <li>2. Enter values to apply for content length comparison: <ul style="list-style-type: none"> <li>– If you select Equal To, Greater Than, or Less Than in the Content Length Operator field, the Content Length Value (Bytes) field appears. In the Content Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are integers from 0 to 4294967295.</li> <li>– If you select Range in the Content Length Operator field, the Content Length Lower Value (Bytes) and the Content Length Higher Value (Bytes) fields appear: <ol style="list-style-type: none"> <li>1. In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value (Bytes) field.</li> <li>2. In the Content Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value (Bytes) field.</li> </ol> </li> </ul> </li> </ol> |

Table 12-12 HTTP Protocol Inspection Match Condition Types (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Header               | <p>The name and value in an HTTP header are to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header.</li> <li>2. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to be matched. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>3. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Header Length        | <p>The length of the header in the HTTP message is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: <ul style="list-style-type: none"> <li>– Request—Indicates that HTTP header request messages are to be checked for header length.</li> <li>– Response—Indicates that HTTP header response messages are to be checked for header length.</li> </ul> </li> <li>2. In the Header Length Operator field, select the operand to be used to compare header length: <ul style="list-style-type: none"> <li>– Equal To—Indicates that the header length must equal the number in the Header Length Value (Bytes) field.</li> <li>– Greater Than—Indicates that the header length must be greater than the number in the Header Length Value (Bytes) field.</li> <li>– Less Than—Indicates that the header length must be less than the number in the Header Length Value (Bytes) field.</li> <li>– Range—Indicates that the header length must be within the range specified in the Header Length Lower Value (Bytes) field and the Header Length Higher Value (Bytes) field.</li> </ul> </li> <li>3. Enter values to apply for header length comparison: <ul style="list-style-type: none"> <li>– If you select Equal To, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value (Bytes) field appears. In the Header Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are integers from 0 to 255.</li> <li>– If you select Range in the Header Length Operator field, the Header Length Lower Value (Bytes) and the Header Length Higher Value (Bytes) fields appear: <ol style="list-style-type: none"> <li>1. In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value (Bytes) field.</li> <li>2. In the Header Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value (Bytes) field.</li> </ol> </li> </ul> </li> </ol> |

Table 12-12 HTTP Protocol Inspection Match Condition Types (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Header MIME Type     | <p>Multipurpose Internet Mail Extension (MIME) message types are to be used for application inspection decisions.</p> <p>In the Header MIME Type field, select the MIME message type to use for this match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Port Misuse          | <p>The misuse of port 80 (or any other port running HTTP) is to be used for application inspection decisions.</p> <p>Indicate the application category to use for this match condition:</p> <ul style="list-style-type: none"> <li>IM—Indicates that instant messaging applications are to be used for this match condition.</li> <li>P2P—Indicates that peer-to-peer applications are to be used for this match condition.</li> <li>Tunneling—Indicates that tunneling applications are to be used for this match condition.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Request Method       | <p>The request method is to be used for application inspection decisions.</p> <p>By default, ACE appliances allow all request and extension methods. This option allows you to configure class maps that define application inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods.</p> <ol style="list-style-type: none"> <li>In the Request Method Type field, select the type of compliance to be used for application inspection decision: <ul style="list-style-type: none"> <li>Ext—Indicates that an HTTP extension method is to be used for application inspection decisions.</li> </ul> <div data-bbox="480 1001 527 1041" data-label="Image"></div> <div data-bbox="472 1041 532 1071" data-label="Section-Header"><b>Note</b></div> <div data-bbox="558 1041 1408 1106" data-label="Text"> <p>The list of available HTTP extension methods from which to choose varies depending on the version of software installed in the ACE.</p> </div> <ul style="list-style-type: none"> <li>RFC—Indicates that a request method defined in RFC 2616 is to be used for application inspection decisions.</li> </ul> <p>Depending on your selection, the Ext Request Method field or the RFC Request Method field appears.</p> </li> <li>In the Request Method field, select the specific request method to be used.</li> </ol> |
| Transfer Encoding    | <p>An HTTP transfer-encoding type is to be used for application inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient.</p> <p>In the Transfer Encoding field, select the type of encoding that is to be checked:</p> <ul style="list-style-type: none"> <li>Chunked—The message body is transferred as a series of chunks.</li> <li>Compress—The encoding format that is produced by the UNIX file compression program compress.</li> <li>Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951.</li> <li>Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952.</li> <li>Identity—The default (identity) encoding which does not require the use of transformation.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                               |



Table 12-12 HTTP Protocol Inspection Match Condition Types (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL                  | <p>URL names are to be used for application inspection decisions.</p> <p>In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <i>www.hostname.domain</i>. For example, in the URL <i>www.anydomain.com/latest/whatsnew.html</i>, include only <i>/latest/whatsnew.html</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| URL Length           | <p>URL length is to be used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>In the URL Length Operator field, select the operand to be used to compare URL length: <ul style="list-style-type: none"> <li>Equal To—Indicates that the URL length must equal the number in the URL Length Value (Bytes) field.</li> <li>Greater Than—Indicates that the URL length must be greater than the number in the URL Length Value (Bytes) field.</li> <li>Less Than—Indicates that the URL length must be less than the number in the URL Length Value (Bytes) field.</li> <li>Range—Indicates that the URL length must be within the range specified in the URL Length Lower Value (Bytes) field and the URL Length Higher Value (Bytes) field.</li> </ul> </li> <li>Enter values to apply for URL length comparison: <ul style="list-style-type: none"> <li>If you select Equal To, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value (Bytes) field appears. In the URL Length Value (Bytes) field, enter the value for comparison. Valid entries are from 1 to 65535 bytes.</li> <li>If you select Range in the URL Length Operator field, the URL Length Lower Value (Bytes) and the URL Length Higher Value (Bytes) fields appear: <ol style="list-style-type: none"> <li>In the URL Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value (Bytes) field.</li> <li>In the URL Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value (Bytes) field.</li> </ol> </li> </ul> </li> </ol> |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.



**Note** If you click **Deploy Now**, the ACE appliance drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to configure another match condition for this class map.

**Related Topics**

- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Setting Match Conditions for Class Maps, page 12-10](#)
- [Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14](#)
- [Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16](#)
- [Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 12-30](#)

## Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps

Use this procedure to set match conditions for a Layer 7 FTP command inspection class map.

**Assumption**

You have configured a Layer 7 command inspection class map and want to establish match criteria.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the Layer 7 FTP command inspection class map that you want to configure match conditions for. You can select multiple class maps (hold down the Shift key while selecting entries) and apply common match conditions to them.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select Request Method Name as the match condition type for this class map.
- Step 6** In the Request Method Name field, select the FTP command to be inspected. [Table 12-13](#) identifies the FTP commands that can be inspected.

**Table 12-13** *FTP Commands for Inspection*

| FTP Command | Description                                                              |
|-------------|--------------------------------------------------------------------------|
| Appe        | Append data to the end of the specified file on the remote host.         |
| Cdup        | Change to the parent of the current directory.                           |
| Cele        | Delete the specified file.                                               |
| Get         | Copy the specified file from the remote host to the local system.        |
| Help        | List all available FTP commands.                                         |
| Mkd         | Create a directory using the specified path and directory name.          |
| Put         | Copy the specified file from the local system to the remote host.        |
| Rmd         | Remove the specified directory.                                          |
| Rnfr        | Rename a file, specifying the current file name. Used with <b>rnfo</b> . |
| Rnfo        | Rename a file, specifying the new file name. Used with <b>rnfr</b> .     |

Table 12-13 FTP Commands for Inspection (continued)

| FTP Command | Description                                                |
|-------------|------------------------------------------------------------|
| Site        | Execute a site-specific command.                           |
| Stou        | Store a file on the remote host and give it a unique name. |
| Syst        | Query the remote host for operating system information.    |

**Step 7** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance and to return to the Match Condition table.



**Note** If you click **Deploy Now**, the ACE appliance drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to configure another match condition for this class map.

#### Related Topics

- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

## Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps

Use this procedure to set match conditions for a SIP deep packet inspection class map.

#### Assumption

You have configured a SIP deep packet inspection class map and want to establish match criteria.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Class Maps**. The Class Maps table appears.
- Step 2** In the Class Maps table, select the SIP deep packet inspection class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, and then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Sequence Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 12-14](#).

**Table 12-14** Layer 7 SIP Deep Packet Inspection Class Map Match Conditions

| Match Condition    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Called Party       | <p>The destination or called party in the URI of the SIP To header is used to establish a match condition.</p> <p>In the Called Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p> |
| Calling Party      | <p>The source or calling party in the URI of the SIP From header is used to establish a match condition.</p> <p>In the Calling Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>  |
| IM Subscriber      | <p>An IM (instant messaging) subscriber is used to establish a match condition.</p> <p>In the IM Subscriber field, enter a regular expression that identifies the IM subscriber for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                                                          |
| Message Path       | <p>A message coming from or transiting through certain SIP proxy servers is used to establish a match condition.</p> <p>In the Message Path field, enter a regular expression that identifies the SIP proxy server for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                       |
| SIP Content Length | <p>The SIP message body length is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Content Operator field, confirm that Greater Than is selected.</li> <li>2. In the Content Length field, enter the maximum size of a SIP message body in bytes that the ACE is to allow without performing SIP protocol inspection. If a SIP message exceeds the specified value, the ACE performs SIP protocol inspection as defined in an associated policy map. Valid entries are integers from 0 to 65534 bytes.</li> </ol>     |
| SIP Content Type   | <p>The content type in the SIP message body is used to establish a match condition.</p> <p>In the Content Type field, enter the a regular expression that identifies the content type in the SIP message body to use for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>                     |
| SIP Request Method | <p>A SIP request method is used to establish a match condition.</p> <p>In the Request Method field, select the request method that is to be matched.</p>                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 12-14 Layer 7 SIP Deep Packet Inspection Class Map Match Conditions (continued)

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Third Party     | <p>A third party who is authorized to register other users on their behalf is used to establish a match condition.</p> <p>In the Third Party Registration Entities field, enter a regular expression that identifies a privileged user authorized for third-party registrations for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</p>  |
| URI Length      | <p>A SIP URI or user identifier is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>In the URI Type field, select the type of URI to use: <ul style="list-style-type: none"> <li>SIP URI—The calling party URI is used for this match condition.</li> <li>Tel URI—A telephone number is used for this match condition.</li> </ul> </li> <li>In the URI Operator field, confirm that Greater Than is selected.</li> <li>In the URI Length field, enter the maximum length of the SIP URI or Tel URI in bytes. Valid entries are integers from 0 to 254 bytes.</li> </ol> |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



**Note** If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Click **Next** to configure another match condition for this class map.

**Related Topics**

- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)

# Configuring Virtual Context Policy Maps

Policy maps establish traffic policy for the ACE appliance. The purpose of a traffic policy is to implement specific ACE appliance functions associated with a traffic class. A traffic policy contains:

- A policy map name.
- A previously created traffic class map or, optionally, the default class map.
- One or more of the individual Layer 3/Layer 4 or Layer 7 policies that specify the actions to be performed by the ACE appliance.

The ACE appliance executes actions specified in a policy map on a first-match, multi-match, or all-match basis:

- **First-match**—With a first-match policy map, the ACE appliance executes only the action specified against the first classification that it matches. Layer 3/Layer 4 Management Traffic, Layer 7 Server Load Balancing, Layer 7 Command Inspection - FTP, and Layer 7 HTTP Optimization policy maps are first-match policy maps.
- **Multi-match**—With a multi-match policy map, the ACE appliance executes all possible actions applicable for a specific classification. Layer 3/Layer 4 Network Traffic policy maps are multi-match policy maps.
- **All-match**—With an all-match policy map, the ACE appliance attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request.


You can view a context's policy maps and their types in the Policy Maps table (**Config > Virtual Contexts > *context* > Expert > Policy Maps**.)

The types of policy maps that you can configure depend on the ACE device type. [Table 12-15](#) lists the types of policy maps with brief descriptions.

**Table 12-15** Policy Maps

| Policy Map                                        | Description                                                                       | Related Topic                                                                                              |
|---------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Layer 3/4 Management Traffic (First-Match)        | Layer 3 and Layer 4 policy map for network management traffic received by the ACE | <a href="#">Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic, page 12-45</a>    |
| Layer 3/4 Network Traffic (Multi-Match)           | Layer 3 and Layer 4 policy map for traffic passing through the ACE                | <a href="#">Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 12-37</a>       |
| Layer 7 Command Inspection - FTP (First-Match)    | Layer 7 policy map for inspection of FTP commands                                 | <a href="#">Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection, page 12-79</a>        |
| Layer 7 Deep Packet Inspection - HTTP (All-Match) | Layer 7 policy map for inspection of HTTP packets                                 | <a href="#">Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 12-73</a>   |
| Layer 7 Deep Packet Inspection - SIP (All-Match)  | Layer 7 policy map for inspection of SIP packets                                  | <a href="#">Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 12-82</a>    |
| Layer 7 Deep Packet Inspection - Skinny           | Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)        | <a href="#">Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection, page 12-84</a> |

Table 12-15 Policy Maps (continued)

| Policy Map                                    | Description                                                                                                                                                                                                                                                                                                                                                 | Related Topic                                                                                              |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Layer 7 HTTP Optimization (First-Match)       | Layer 7 policy map for optimizing HTTP traffic                                                                                                                                                                                                                                                                                                              | <a href="#">Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 12-86</a>             |
| Layer 7 Server Load Balancing (First-Match)   | Layer 7 policy map for HTTP server load balancing                                                                                                                                                                                                                                                                                                           | <a href="#">Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46</a> |
| Server Load Balancing - Generic (First-Match) | Generic Layer 7 policy map for server load balancing                                                                                                                                                                                                                                                                                                        | <a href="#">Setting Policy Map Rules and Actions for Generic Server Load Balancing, page 12-54</a>         |
| Server Load Balancing - HTTPS (First-Match)   | Layer 7 policy map for HTTPS server load balancing<br> <b>Note</b> The SLB HTTPS (First-Match) option is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2). | <a href="#">Setting Policy Map Rules and Actions for HTTPS Server Load Balancing, page 12-58</a>           |
| Server Load Balancing - RADIUS (First-Match)  | Layer 7 policy map for RADIUS server load balancing                                                                                                                                                                                                                                                                                                         | <a href="#">Setting Policy Map Rules and Actions for RADIUS Server Load Balancing, page 12-63</a>          |
| Server Load Balancing - RDP (First-Match)     | Layer 7 policy map for RDP server load balancing                                                                                                                                                                                                                                                                                                            | <a href="#">Setting Policy Map Rules and Actions for RDP Server Load Balancing, page 12-71</a>             |
| Server Load Balancing - RTSP (First-Match)    | Layer 7 policy map for RTSP server load balancing                                                                                                                                                                                                                                                                                                           | <a href="#">Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 12-65</a>            |
| Server Load Balancing - SIP (First-Match)     | Layer 7 policy map for SIP server load balancing                                                                                                                                                                                                                                                                                                            | <a href="#">Setting Policy Map Rules and Actions for SIP Server Load Balancing, page 12-68</a>             |

Use this procedure to create a policy map for a virtual context.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** Click **Add** to add a new policy map, or select an existing policy map, and then click **Edit** to modify it.
- Step 3** The Policy Map Name field contains an automatically incremented number for the policy map. Either leave the entry as it is or enter a different, unique number.
- Step 4** In Type, select the type of policy map to create. See [Table 12-15](#) for a list of policy maps.
- Step 5** In the Description field, enter a brief description of the policy map.
- Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. To define rules and actions for this policy map, see [Configuring Rules and Actions for Policy Maps, page 12-36](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save your entries and to configure another policy map.

#### Related Topics

- [Using Virtual Contexts, page 4-2](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Real Servers, page 6-5](#)
- [Configuring Server Farms, page 6-18](#)
- [Configuring Sticky Groups, page 7-11](#)

## Configuring Rules and Actions for Policy Maps


Table 12-16 lists the policy maps and related topics for setting rules and actions.

**Table 12-16** Topic Reference for Policy Map Rules and Actions

| Policy Map Type                                   | Topic for Setting Rules and Actions                                                                        |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Layer 3/4 Management Traffic (First-Match)        | <a href="#">Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic, page 12-45</a>    |
| Layer 3/4 Network Traffic (First-Match)           | <a href="#">Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 12-37</a>       |
| Layer 7 Command Inspection - FTP (First-Match)    | <a href="#">Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection, page 12-79</a>        |
| Layer 7 Deep Packet Inspection - HTTP (All-Match) | <a href="#">Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 12-73</a>   |
| Layer 7 Deep Packet Inspection - SIP (All-Match)  | <a href="#">Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 12-82</a>    |
| Layer 7 Deep Packet Inspection - Skinny           | <a href="#">Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection, page 12-84</a> |
| Layer 7 HTTP Optimization (First-Match)           | <a href="#">Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 12-82</a>    |
| Layer 7 Server Load Balancing (First-Match)       | <a href="#">Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46</a> |
| Server Load Balancing - Generic (First-Match)     | <a href="#">Setting Policy Map Rules and Actions for Generic Server Load Balancing, page 12-54</a>         |



Table 12-16 Topic Reference for Policy Map Rules and Actions (continued)

| Policy Map Type                              | Topic for Setting Rules and Actions                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Load Balancing - HTTPS (First-Match)  | <a href="#">Setting Policy Map Rules and Actions for HTTPS Server Load Balancing, page 12-58</a><br> <b>Note</b> The SLB HTTPS (First Match) feature does not apply to the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2). |
| Server Load Balancing - RADIUS (First-Match) | <a href="#">Setting Policy Map Rules and Actions for RADIUS Server Load Balancing, page 12-63</a>                                                                                                                                                                                                                                                                                                      |
| Server Load Balancing - RDP (First-Match)    | <a href="#">Setting Policy Map Rules and Actions for RDP Server Load Balancing, page 12-71</a>                                                                                                                                                                                                                                                                                                         |
| Server Load Balancing - RTSP (First-Match)   | <a href="#">Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 12-65</a>                                                                                                                                                                                                                                                                                                        |
| Server Load Balancing - SIP (First-Match)    | <a href="#">Setting Policy Map Rules and Actions for SIP Server Load Balancing, page 12-68</a>                                                                                                                                                                                                                                                                                                         |

## Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic

Use this procedure to configure the rules and actions for Layer 3/Layer 4 traffic other than network management traffic.

### Assumptions

- You have configured a Layer 3/Layer 4 policy map.
- A class map has been defined if you do not want to use the class-default or class-default-v6 class map.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the Layer 3/Layer 4 network traffic policy map you want to set rules and actions for, and then select the Rule tab.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule configuration screen appears.
- Step 4** In the Type field, confirm that Class Map is selected.
- Step 5** In the Use Class Map field:
  - For an IPv6 default class map, select the class-default radio button.
  - For an IPv6 default class map, select the class-default-v6 radio button.
  - For a previously created class map, go to the next step.

- Step 6** To use a previously created class map for this rule, perform the following
- In the Use Class Map field, select the others radio button.
  - In the Class Map Name field, select the class map to be used.
  - In the Insert Before field, indicate whether this rule is to precede another rule in this policy map:
    - N/A—Indicates that this option is not configured.
    - False—Indicates that this rule is not to precede another rule in this policy map.
    - True—Indicates that this rule is to precede another rule in this policy map.
  - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 7** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance and to define actions for this rule (see [Step 8](#)).
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
  - Click **Next** to save your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 6](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

- Click the Rule tab to refresh the Rule table.
- In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 8** To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.
- Step 9** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- Step 10** In the Action Type field, select the type of action to be taken for this rule, and then configure the related attributes. See [Table 12-17](#).

**Table 12-17** Layer 3/Layer 4 Network Traffic Policy Map Actions

| Action                 | Description/Steps                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appl-Parameter-DNS     | A DNS parameter map containing DNS-related actions is to be implemented for this rule.<br>In the Parameter Map field, specify the name of the DNS parameter map to use.     |
| Appl-Parameter-Generic | A generic parameter map is to be implemented for this rule.<br>In the Parameter Map field, specify the name of the generic parameter map to use.                            |
| Appl-Parameter-HTTP    | An HTTP parameter map containing HTTP-related actions is to be implemented for this rule.<br>In the Parameter Map field, specify the name of the HTTP parameter map to use. |
| Appl-Parameter-RDP     | An RDP parameter map containing RDP-related actions is to be implemented for this rule.<br>In the Parameter Map field, specify the name of the RDP parameter map to use.    |

**Table 12-17**      *Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)*

| Action                | Description/Steps                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appl-Parameter-RTSP   | An RTSP parameter map containing RTSP-related actions is to be implemented for this rule.<br>In the Parameter Map field, specify the name of the RTSP parameter map to use.                                                                                                                                                                       |
| Appl-Parameter-SIP    | A SIP parameter map containing SIP-related actions is to be implemented for this rule.<br>In the Parameter Map field, specify the name of the SIP parameter map to use.                                                                                                                                                                           |
| Appl-Parameter-Skinny | A Skinny parameter map containing Skinny-related actions is to be implemented for this rule.<br>In the Parameter Map field, specify the name of the Skinny parameter map to use.                                                                                                                                                                  |
| Connection            | A connection parameter map containing TCP/IP connection-related commands that pertain to normalization and termination is to be implemented for this rule.<br>In the Connection Parameter Maps field, select the Connection parameter map that is to be used.                                                                                     |
| HTTP Optimize         | In the HTTP Optimization Policy field, select the HTTP optimization policy map to use.                                                                                                                                                                                                                                                            |
| Inspect               | Application inspection is to be implemented for this rule.<br><ol style="list-style-type: none"> <li>1. In the Inspect Type field, select the protocol that is to be inspected.</li> <li>2. Provide any protocol-specific information.</li> </ol> <a href="#">Table 12-18</a> describes the available options for application inspection actions. |

Table 12-17 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

| Action | Description/Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NAT    | <p>The ACE is to implement network address translation (NAT) for this rule.</p> <ol style="list-style-type: none"> <li>In the NAT Mode field, select the type of NAT to be used: <ul style="list-style-type: none"> <li>Dynamic NAT—NAT is to translate local addresses to a pool of global addresses. Continue with Step 3.</li> <li>Static NAT—NAT is to translate each local address to a fixed global address. Continue with Step 2.</li> </ul> </li> <li>If you select Static NAT, do the following: <ol style="list-style-type: none"> <li>For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>In the Static Mapped v4 or v6 Address field, enter the IP address to use for static NAT translation. This entry establishes the globally unique IP address of a host as it appears to the outside world. The policy map performs the global IP address translation for the source IP address specified in the ACL (as part of the class-map traffic classification).</li> <li>For an IPv4 address, in the Static Mapped Netmask field, select the subnet mask to apply to the static mapped address.<br/><br/>For an IPv6 address, in the Static Mapped Prefix-length field, enter the prefix length for the static mapped address.</li> <li>In the NAT Protocol field, select the protocol to use for NAT: <ul style="list-style-type: none"> <li>- N/A—This attribute is not set.</li> <li>- TCP—The ACE is to use TCP for NAT.</li> <li>- UDP—The ACE is to use UDP for NAT.</li> </ul> </li> <li>In the Static Port field, enter the TCP or UDP port to use for static port redirection. Valid entries are integers from 0 to 65535.</li> <li>In the VLAN Id field, select the VLAN to use for NAT.</li> </ol> </li> <li>If you select Dynamic NAT, do the following: <ol style="list-style-type: none"> <li>In the NAT Pool Id field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are integers from 1 to 2147483647. See <a href="#">Configuring VLAN Interface NAT Pools and Displaying NAT Utilization</a>, page 10-32.</li> <li>In the VLAN Id field, select the VLAN to use for NAT.</li> </ol> </li> </ol> <p><b>Note</b> For dynamic NAT, ACE allows you to associate a non-configured NAT pool ID to the dynamic NAT action. However, the ANM will not discover the dynamic NAT action when the NAT pool ID is not configured. You must associate the configured NAT pool ID to the dynamic NAT action for ANM discovery to complete successfully.</p> |

Table 12-17 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)


| Action                        | Description/Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kal-ap-Primary-Out-of-Service | <p>Enables the ACE to notify the Global Site Selector (GSS) that the primary server farm is down when the backup server farm is in use.</p> <p>By default, when you configure a redirect server farm as a backup server farm on the ACE and the primary server farm fails, the backup server farm redirects the client requests to another data center. However, the VIP remains in the INSERVICE state.</p> <p>When you configure the ACE to communicate with a Global Site Selector (GSS), it provides information for server availability. When a backup server is in use after the primary server farm is down, this feature enables the ACE to inform the GSS that the VIP for the primary server farm is out of service by returning a load value of 255. The GSS recognizes that the primary server farm is down and sends future DNS requests with the IP address of the other data center.</p> |
| Policymap                     | <p>The ACE is to associate a Layer 7 server load-balancing policy map with this Layer 3/Layer 4 policy map.</p> <p>In the Policy Map field, select the Layer 7 policy map to associate with this Layer 3/Layer 4 policy map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSL-Proxy                     | <p> <b>Note</b> The SSL-Proxy option is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> <p>The ACE is to use an SSL proxy server service to define the SSL parameters the ACE is to use during the handshake and subsequent SSL session.</p> <ol style="list-style-type: none"> <li>1. In the SSL Proxy field, select the SSL proxy server service to use in the handshake and subsequent SSL session when the ACE engages with an SSL client.</li> <li>2. In the SSL Proxy Type field, confirm that Server is selected to indicate that the ACE is to be configured so that it is recognized as an SSL server.</li> </ol>                                                                       |
| UDP-Fast-Age                  | The ACE is to close the connection immediately after sending a response to the client, thereby enabling per-packet load balancing for UDP traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| VIP-ICMP-Reply                | <p>A VIP is to send an ICMP ECHO-REPLY response to ICMP requests.</p> <ol style="list-style-type: none"> <li>1. In the Active field, click the check box to instruct the ACE to reply to an ICMP request only if the configured VIP is active. If the VIP is not active and the active option is specified, the ACE discards the ICMP request and the request times out.</li> <li>2. In the Primary Inservice field, click the check box to instruct the ACE to reply to an ICMP ping only if the primary server farm state is UP, regardless of the state of the backup server farm. If this option is enabled and the primary server farm state is DOWN, the ACE discards the ICMP request and the request times out.</li> </ol>                                                                                                                                                                      |

Table 12-17 Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)

| Action         | Description/Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VIP-In-Service | A VIP is to be enabled for server load-balancing operations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| KAL-AP-TAG     | <p>The KAL-AP-TAG feature allows the Cisco Global Site Selector (GSS) proprietary KAL-AP protocol to extract load and availability information from the ACE when a firewall is positioned between the GSS and the ACE. This feature allows you to configure a tag (name) per VIP for a maximum of 4,096 tags on an ACE. This feature does not replace the tag per domain feature. For more information about this feature, see the Configuring Health Monitoring chapter in the <i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i>.</p> <p><b>Note</b> The KAL-AP-TAG selection is not available for the class-default class map.</p> <p>In the KAL-AP-Tag Name field, enter the name as an unquoted text string with no spaces and a maximum of 76 alphanumeric characters.</p> <p>The following scenarios are not supported and will result in an error:</p> <ul style="list-style-type: none"> <li>You cannot configure a tag name for a VIP that already has a tag configuration as part of a different policy configuration.</li> <li>You cannot associate the same tag name with more than one VIP.</li> <li>You cannot associate the same tag name with a domain and a VIP.</li> <li>You cannot assign two different tags to two different Layer 3 class maps that have the same VIP, but different port numbers. The KAL-AP protocol considers these class maps to have the same VIP and calculates the load for both Layer 3 rules together when the GSS queries the VIP.</li> </ul> |

**Table 12-18** Policy Map Application Inspection Options

| Inspection Option | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DNS               | <p>Indicates that Domain Name System (DNS) query inspection is to be implemented. DNS requires application inspection so that DNS queries will not be subject to the generic UDP handling based on activity timeouts. Instead, the UDP connections associated with DNS queries and responses are torn down as soon as a reply to a DNS query has been received. The ACE appliance performs the reassembly of DNS packets to verify that the packet length is less than the configured maximum length.</p> <p>In the DNS Max. Length field, enter the maximum length of a DNS reply in bytes. Valid entries are integers from 512 to 65535.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| FTP               | <p>Indicates that FTP inspection is to be implemented. The ACE appliance inspects FTP packets, translates the address and port embedded in the payload, and opens up secondary channel for data.</p> <ol style="list-style-type: none"> <li>1. In the Parameter Map field, specify a previously created parameter map used to define parameters for FTP inspection.</li> <li>2. In the FTP Strict field, indicate whether the ACE appliance is to check for protocol RFC compliance and prevent Web browsers from sending embedded commands in FTP requests: <ul style="list-style-type: none"> <li>– N/A—Indicates that this attribute is not set.</li> <li>– False—Indicates that the ACE appliance is not to check for RFC compliance or prevent Web browsers from sending embedded commands in FTP requests.</li> <li>– True—Indicates that the ACE appliance is to check for RFC compliance and prevent Web browsers from sending embedded commands in FTP requests.</li> </ul> </li> <li>3. If you select True, in the FTP Inspect Policy field, select the Layer 7 FTP command inspection policy to be implemented for this rule.</li> </ol>                                                                                        |
| HTTP              | <p>Indicates that enhanced Hypertext Transfer Protocol (HTTP) inspection is to be performed on HTTP traffic. The inspection checks are based on configured parameters in an existing Layer 7 policy map and internal RFC compliance checks performed by the ACE appliance. By default, the ACE appliance allows all request methods.</p> <ol style="list-style-type: none"> <li>1. In the HTTP Inspect Policy field, select the HTTP inspection policy map to be implemented for this rule. If you do not specify a Layer 7 policy map, the ACE appliance performs a general set of Layer 3 and Layer 4 protocol fixup actions and internal RFC compliance checks.</li> <li>2. In the URL Logging field, indicate whether Layer 3 and Layer 4 traffic is to be monitored: <ul style="list-style-type: none"> <li>– N/A—Indicates that this attribute is not set.</li> <li>– False—Indicates that Layer 3 and Layer 4 traffic is not to be monitored.</li> <li>– True—Indicates that Layer 3 and Layer 4 traffic is to be monitored. When enabled, this function logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed.</li> </ul> </li> </ol> |

Table 12-18 Policy Map Application Inspection Options (continued)

| Inspection Option | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICMP              | <p>Indicates that Internet Control Message Protocol (ICMP) payload inspection is to be performed. ICMP inspection allows ICMP traffic to have a “session” so it can be inspected similarly to TCP and UDP traffic.</p> <p>In the ICMP Error field, indicate whether the ACE appliance is to perform name address translation on ICMP error messages:</p> <ul style="list-style-type: none"> <li>• N/A—Indicates that this attribute is not set.</li> <li>• False—Indicates that the ACE appliance is not to perform NAT on ICMP error messages.</li> <li>• True—Indicates that the ACE appliance is to perform NAT on ICMP error messages. When enabled, the ACE appliance creates translation sessions for intermediate or endpoint nodes that send ICMP error messages based on the NAT configuration. The ACE appliance overwrites the packet with the translated IP addresses.</li> </ul> |
| ILS               | Internet Locator Service (ILS) protocol inspection is to be implemented.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| RTSP              | Indicates that Real Time Streaming Protocol (RTSP) packet inspection is to be implemented. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. The ACE appliance monitors Setup and Response (200 OK) messages in the control channel established using TCP port 554 (no UDP support).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SIP               | <p>SIP protocol inspection is implemented. SIP is used for call handling sessions and instant messaging. The ACE inspects signaling messages for media connection addresses, media ports, and embryonic connections. The ACE also uses NAT to translate IP addresses that are embedded in the user-data portion of the packet.</p> <ol style="list-style-type: none"> <li>1. In the Parameter Map field, specify a previously created parameter map used to define parameters for SIP inspection.</li> <li>2. In the SIP Inspect Policy field, select a previously created Layer 7 SIP inspection policy map to implement packet inspection of Layer 7 SIP application traffic.</li> </ol> <p>If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.</p>                                    |
| Skinny            | <p>Cisco Skinny Client Control Protocol (SCCP) protocol inspection is implemented. The SCCP is a Cisco proprietary protocol that is used between Cisco CallManager and Cisco VOiP phones. The ACE uses NAT to translate embedded IP addresses and port numbers in SCCP packet data.</p> <ol style="list-style-type: none"> <li>1. In the Parameter Map field, specify a previously created connection parameter map used to define parameters for Skinny inspection.</li> <li>2. In the Skinny Inspect Policy field, select a previously created Layer 7 Skinny inspection policy map to implement packet inspection of Layer 7 Skinny application traffic.</li> </ol> <p>If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.</p>                                                        |

**Step 11** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.
- Click **Next** to save your entries and to configure another Action.



**Related Topics**

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic

Use this procedure to configure the rules and actions for IP management traffic received by the ACE appliance.

**Assumptions**

- A network management policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default or class-default-v6 class map.

**Procedure**

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the Layer 3/Layer 4 management traffic policy map you want to set rules and actions for, and then select the **Rule** tab. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
- Step 4** In the Type field, confirm that Class Map is selected.
- Step 5** In the Use Class Map field:
- For an IPv4 default class map, select the class-default radio button.
  - For an IPv6 default class map, select the class-default-v6 radio button.
  - For a previously created class map, go to the next step.
- Step 6** To use a previously created class map for this rule:
- In the Use Class Map field, select the others radio button.
  - In the Class Map Name field, select the class map to be used.
  - In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.
    - N/A—Indicates that this option is not configured.
    - False—Indicates that this rule is not to precede another rule in this policy map.
    - True—Indicates that this rule is to precede another rule in this policy map.
  - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 7** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with [Step 8](#).

- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 6](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 8** To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

**Step 9** In the Action configuration screen:

- a. In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- b. In the Action Type field, select **Mgmt-permit** to indicate that this action permits or denies network management traffic.
- c. In the Action field, specify the action that is to occur:
  - Deny—Indicates that the ACE appliance is to deny network management traffic when this rule is met.
  - Permit—Indicates that the ACE appliance is to accept network management traffic when this rule is met.

**Step 10** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to save your entries and to configure another action.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic

Use this procedure to set rules and actions for Layer 7 server load-balancing policy maps.

### Assumptions

- You have configured a load-balancing policy map and want to establish the corresponding rules and actions.
- If you want to configure an SSL proxy action, you have configured SSL proxy service for this context.
- If you want to insert, rewrite, and delete HTTP headers, ensure that an HTTP header modify action list has been configured. See [Configuring an HTTP Header Modify Action List, page 12-90](#) for more information.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the load-balancing policy map you want to set rules and actions for, and then select the Rule tab. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.
- Step 4** Select the type of rule to be used:
- **Class Map**—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions. If you select this rule type, continue with [Step 5](#).
  - **Match Condition**—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions. If you select this rule type, continue with [Step 6](#).
- Step 5** If you select Class Map, either check the Use Class Default check box to use a default class map or specify a previously created class map:
- a. Clear the Use Class Default check box.
  - b. In the Class Map Name field, select the class map to be used.
  - c. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.
    - N/A—Indicates that this option is not configured.
    - False—Indicates that this rule is not to precede another rule in this policy map.
    - True—Indicates that this rule is to precede another rule in this policy map.
  - d. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 6** For match conditions:
- a. In the Match Condition Name field enter a name for the match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
  - b. In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See [Table 12-19](#) for information about these selections.


Table 12-19 Policy Match Condition Types

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP Content    | <p>Specific content contained within the HTTP entity-body is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 4000.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| HTTP Cookie     | <p>Indicates that HTTP cookies are to be used for this rule.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching string expressions. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| HTTP Header     | <p>Indicates that the HTTP header and a corresponding value are to be used for this rule.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the Header Name field, enter the name of the generic field in the HTTP header. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>2. In the Header Value (Bytes) field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. To include spaces, enclose the entire string in quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| HTTP URL        | <p>Indicates that this rule is to perform regular expression matching against the received packet data from a particular connection based on the HTTP URL string.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>1. In the URL Expression field, enter a URL, or portion of a URL, to match. Valid entries are URL strings from 1 to 255 alphanumeric characters. Include only the portion of the URL following <code>www.hostname.domain</code> in the match statement. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>. To match the <code>www.anydomain.com</code> portion, the URL string can take the form of a URL regular expression. The ACE appliance supports regular expressions for matching URL strings. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> <li>2. In the Method Expression field, enter the HTTP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).</li> </ol> |

Table 12-19 Policy Match Condition Types (continued)

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source Address  | <p>Indicates that this rule is to use a client source IP address to establish match conditions.</p> <p>If you select this method:</p> <ol style="list-style-type: none"><li>1. For the IP Address Type, select either IPv4 or IPv6 for the address type.</li><li>2. In the Source IP Address field, enter the source IP address of the client in the format based on the address type (IPv4 or IPv6).</li><li>3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.</li></ol> <p>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</p> |

Table 12-19 Policy Match Condition Types (continued)

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSL             | <p>Defines load balancing decisions based on the specific SSL cipher or cipher strength.</p> <p> <b>Note</b> The SSL option is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> <p>Enables the ACE to load balance client traffic to different server farms based on the SSL encryption level negotiated with the ACE during SSL termination.</p> <p>If you select this method:</p> <ol style="list-style-type: none"> <li>In the SSL Cipher Match Type field, select the match type. Options include: <ul style="list-style-type: none"> <li>Equal To—Specifies an SSL cipher for the load balancing decision.</li> <li>Less Than—Specifies SSL cipher strength for the load balancing decision.</li> </ul> </li> <li>If you selected Equal To, in the Cipher Name field specify an SSL cipher for the load balancing decision. The possible values are as follows: <ul style="list-style-type: none"> <li>RSA_EXPORT1024_WITH_DES_CBC_SHA</li> <li>RSA_EXPORT1024_WITH_RC4_56_MD5</li> <li>RSA_EXPORT1024_WITH_RC4_56_SHA</li> <li>RSA_EXPORT_WITH_DES40_CBC_SHA</li> <li>RSA_EXPORT_WITH_RC4_40_MD5</li> <li>RSA_WITH_3DES_EDE_CBC_SHA</li> <li>RSA_WITH_AES_128_CBC_SHA</li> <li>RSA_WITH_AES_256_CBC_SHA</li> <li>RSA_WITH_DES_CBC_SHA</li> <li>RSA_WITH_RC4_128_MD5</li> <li>RSA_WITH_RC4_128_SHA</li> </ul> </li> <li>If you selected Less Than, in the Specify Minimum Cipher Strength field specify a non-inclusive minimum SSL cipher bit strength. For example, if you specify a cipher strength value of 128, any SSL cipher that was no greater than 128 would hit the traffic policy. If the SSL cipher was 128-bit or greater, the connection would miss the policy.</li> </ol> <p>The possible values are as follows:</p> <ul style="list-style-type: none"> <li>56—56-bit strength</li> <li>128—128-bit strength</li> <li>168—168-bit strength</li> <li>256—256-bit strength</li> </ul> |

**Step 7** For specific class maps and match conditions, in the Insert Before field, indicate whether this rule is to precede another defined policy rule:

- N/A—Indicates that this option is not applicable.
- False—Indicates that this rule is not to precede another defined policy rule.
- True—Indicates that this rule is to precede another policy rule.

If you select True, in the Insert Before Policy Rule field, select the policy rule that this rule is to precede.

**Step 8** Do the following:

- Click **Deploy Now** to deploy the configuration on the ACE appliance. The Action table appears below the Rule table. To define the actions for this rule, continue with [Step 9](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to save your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 7](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 9** In the Action table, click **Add** to add a new action for this rule, or select an existing action, and then click **Edit** to modify it.

**Step 10** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

**Step 11** In the Action tab in the Action Type field, select the action to be taken and configure any action-specific attributes as described in [Table 12-20](#).

**Table 12-20** Policy Map Actions for Load Balancing


| Action      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action      | <p>Indicates that the ACE appliance is to use an HTTP header modify action list to insert, rewrite, or delete HTTP headers. It can also be used to configure the SSL URL rewrite function</p> <p>The Action List drop down appears, listing the configured HTTP header modify action lists (see the <a href="#">“Configuring an HTTP Header Modify Action List”</a> section on page 12-90). Make a selection from this list.</p> <p>If necessary, click <b>Add</b> to add a new HTTP header modify action list, or select an existing action list, and then click <b>Edit</b> to modify it.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Compress    | <p>Indicates that the ACE appliance is to compress packets that match this policy map. This option is available only when you associate an HTTP-type class map with a policy map.</p> <p>In the Compress Method field, specify the method that the ACE appliance is to use to compress packets:</p> <ul style="list-style-type: none"> <li>Deflate—Indicates that the ACE appliance is to use the DEFLATE compression method when the client browser supports both the DEFLATE and GZIP compression methods.</li> <li>Gzip—Indicates that ACE appliance is to use the GZIP compression method when the client browser supports both the DEFLATE and GZIP compression methods. This is the default setting.</li> </ul>                                                                                                                                                                                                                                                                                                                                    |
| Drop        | <p>Indicates that the ACE appliance is to discard packets that match this policy map.</p> <p>In the Action Log field, specify whether the dropped packets are to be logged in the software.</p> <ul style="list-style-type: none"> <li>N/A—This option is not configured.</li> <li>False—Dropped packets are not to be logged in the software.</li> <li>True—Dropped packets are to be logged in the software.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Forward     | Indicates that the ACE appliance is to forward requests that match this policy map without load balancing the requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Insert-HTTP | <p>Indicates that the ACE appliance is to insert an HTTP header for Layer 7 load balancing for requests that match this policy map.</p> <p>This option allows the ACE appliance to identify a client whose IP address has been translated using NAT by inserting a generic header and string value in the client HTTP request.</p> <ol style="list-style-type: none"> <li>In the HTTP Header Name field, enter the name of the generic field in the HTTP header. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>In the HTTP Header Value field, enter the value to be inserted into the HTTP header. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. To include spaces, enclose the entire string in quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol> |



Table 12-20 Policy Map Actions for Load Balancing (continued)

| Action          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reverse Sticky  | <p>Reverse IP stickiness is an enhancement to regular stickiness and is used mainly in firewall load balancing (FWLB). It ensures that multiple distinct connections that are opened by hosts at both ends (client and server) are load-balanced and stuck to the same firewall. Reverse stickiness applies to such protocols as FTP, RTSP, SIP, and so on where there are separate control channels and data channels opened by the client and the server, respectively. For complete details about reverse stickiness, see the <i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i>.</p> <p>In the Sticky Group field, choose the name of an existing IPv4 IP netmask or IPv6 prefix sticky group that you want to associate with reverse IP stickiness.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Server Farm     | <p>Indicates that the ACE appliance is to load balance client requests for content to a server farm.</p> <ol style="list-style-type: none"> <li>1. In the Server Farm field, select the server farm to which requests for content are to be sent.</li> <li>2. In the Backup Server Farm field, select the backup server farm to which requests for content are to be sent.<br/>Leave this field blank to indicate that no backup server farm is to be used.</li> <li>3. Check the Sticky Enabled check box to indicate that the sticky group associated with this policy and applied to the primary server farm is applied to the backup server farm. Clear the Sticky Enabled check box to indicate that the sticky group associated with this policy and applied to the primary server farm in that policy is not applied to the backup server farm.</li> <li>4. Check the Aggregate State Enabled check box to indicate that the operational state of the backup server farm is taken into consideration when evaluating the state of the load-balancing class in a policy map. Clear this check box to indicate that the operational state of the backup server farm is not taken into consideration when evaluating the state of the load-balancing class in a policy map.</li> </ol> |
| Server Farm-NAT | <p>The ACE is to apply dynamic NAT to traffic for this policy map.</p> <ol style="list-style-type: none"> <li>1. In the NAT Pool ID field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are integers from 1 to 2147483647. For information on configuring NAT pools, see <a href="#">Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32</a>.</li> <li>2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 to 4094.</li> <li>3. In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Set-IP-TOS      | <p>The ACE is to set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings.</p> <p>In the IP TOS Rewrite Value (Bytes) field, enter the IP DSCP value. Valid entries are integers from 0 to 255.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Table 12-20 Policy Map Actions for Load Balancing (continued)

| Action             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSL-Proxy          |  <p><b>Note</b> The SSL-Proxy action is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> <p>Indicates that the ACE appliance is to use an SSL proxy client service to define the SSL parameters the ACE appliance is to use during the handshake and subsequent SSL session.</p> <ol style="list-style-type: none"> <li>1. In the SSL Proxy field, select the SSL proxy server service to be used for this action.</li> <li>2. In the SSL Proxy Type field, select Client to indicate that the ACE appliance is to be configured so that it is recognized as an SSL client.</li> </ol> |
| Sticky-Server Farm | <p>Indicates that requests matching this policy map be load balanced to a sticky server farm.</p> <p>In the Sticky Group field, select the sticky server farm that is to be used for requests that match this policy map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Step 12** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to save your entries and to configure another action.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Generic Server Load Balancing

Use this procedure to configure the rules and actions for generic traffic received by the ACE.

#### Assumptions

- A generic traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the generic traffic policy map you want to set rules and actions for. The Rule table appears.

- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
- Step 4** In the Type field, configure rules using the information in [Table 12-21](#).

**Table 12-21** Generic Server Load Balancing Policy Map Rules

| Option    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map | <p>A class map is used for this traffic policy.</p> <ol style="list-style-type: none"><li>To use the class-default class map, check the Use Class Default check box.<br/>The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit <b>match any</b> statement that enables it to match all traffic.</li><li>To use a previously created class map:<ol style="list-style-type: none"><li>Clear the Use Class Default check box.</li><li>In the Class Map Name field, select the class map to be used.</li></ol></li></ol> |

Table 12-21 Generic Server Load Balancing Policy Map Rules (continued)

| Option          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Match Condition | A match condition is used for this traffic policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                 | Match Condition Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                 | Match Condition Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Layer 4 Payload                                                                                                                            | <p>Layer 4 payload data is used for the network matching criteria.</p> <ol style="list-style-type: none"> <li>1. In the Layer 4 Payload RegexMatch Condition field, enter a Layer 4 payload expression that is contained within the TCP or UDP entity body. Valid entries are strings containing 1 to 255 alphanumeric characters. <a href="#">Table 12-33</a> lists the supported characters that you can use for matching string expressions.</li> <li>2. In the Layer 4 Payload Offset field, enter the absolute offset in the data where the Layer 4 payload expression search string starts. The offset starts at the first byte of the TCP or UDP body. Valid entries are integers from 0 to 999.</li> </ol> |
|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Source Address                                                                                                                             | <p>A client source host IPv4 address and subnet mask, or IPv6 address and prefix length are used for the network traffic matching criteria.</p> <ol style="list-style-type: none"> <li>1. For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>2. In the Source IP Address field, enter the source IP address of the client in the format based on the address type (IPv4 or IPv6).</li> <li>3. For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.</li> </ol> <p>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</p>                                                         |
| Insert Before   | <ol style="list-style-type: none"> <li>1. Indicate whether this rule is to precede another rule for this policy map. <ul style="list-style-type: none"> <li>– N/A—This option is not configured.</li> <li>– False—This rule is not to precede another rule in this policy map.</li> <li>– True—This rule is to precede another rule in this policy map.</li> </ul> </li> <li>2. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.</li> </ol> |                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with [Step 6](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.



**Note** If you selected the Insert Before option and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 6** In the Action table, click **Add** to add an entry or select an existing entry to modify, and then click **Edit**.

**Step 7** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

**Step 8** In the Action Type field, configure actions for this rule using the information in [Table 12-22](#).

**Table 12-22** Generic Server Load Balancing Policy Map Actions

| Action         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Drop           | The ACE is to discard packets that match this policy map.<br>In the Action Log field, specify whether the dropped packets are to be logged in the software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Forward        | The ACE is to forward the traffic that match this policy map to its destination.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Reverse Sticky | Reverse IP stickiness is an enhancement to regular stickiness and is used mainly in FWLB. It ensures that multiple distinct connections that are opened by hosts at both ends (client and server) are load-balanced and stuck to the same firewall. Reverse stickiness applies to such protocols as FTP, RTSP, SIP, and so on where there are separate control channels and data channels opened by the client and the server, respectively. For complete details about reverse stickiness, see the <i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i> .<br>In the Sticky Group field, choose an existing IPv4 IP netmask or IPv6 prefix sticky group that you want to associate with reverse IP stickiness.                                                                                                                                                                 |
| Server Farm    | The ACE is to load balance client requests for content to a server farm.<br><ol style="list-style-type: none"> <li>1. In the Server Farm field, select the server farm for this policy map action.</li> <li>2. In the Backup Server Farm field, select the backup server farm for this action.</li> <li>3. Check the Sticky Enabled check box to indicate that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky.</li> <li>4. Check the Aggregate State Enabled check box to indicate that the operational state of the backup server farm is taken into consideration when evaluating the state of the load-balancing class in a policy map. Clear this check box to indicate that the operational state of the backup server farm is not taken into consideration when evaluating the state of the load-balancing class in a policy map.</li> </ol> |

Table 12-22 Generic Server Load Balancing Policy Map Actions (continued)

| Action             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Farm-NAT    | <p>The ACE is to apply dynamic NAT to traffic for this policy map.</p> <ol style="list-style-type: none"> <li>1. In the NAT Pool ID field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are integers from 1 to 2147483647. For information on configuring NAT pools, see <a href="#">Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32</a>.</li> <li>2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 to 4094.</li> <li>3. In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.</li> </ol> |
| Set-IP-TOS         | <p>The ACE is to set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings.</p> <p>In the IP TOS Rewrite Value (Bytes) field, enter the IP DSCP value. Valid entries are integers from 0 to 255.</p>                                                                                                                                                                                                                                                                                                                                          |
| Sticky Group       | Sticky group that you want to associate with reverse stickiness.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Sticky-Server Farm | <p>The ACE is to load balance client requests for content to a sticky server farm.</p> <p>In the Sticky Group field, select the sticky server farm that is to be used for requests that match this policy map.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 9** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to deploy your entries and to configure another action.

**Related Topics**

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for HTTPS Server Load Balancing

Use this procedure to configure the rules and actions for HTTPS traffic received by the ACE.

**Note**

The HTTPS server load balancing feature does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

**Assumptions**

- An HTTPS traffic policy map has been configured.

- A class map has been defined for a class map rule if you do not want to use the class-default class map.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the HTTPS traffic policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
- Step 4** In the Type field, configure rules using the information in [Table 12-21](#).

**Table 12-23** *HTTPS Server Load Balancing Policy Map Rules*

| Option          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                            |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>A class map is used for this traffic policy.</p> <ol style="list-style-type: none"> <li>1. To use the class-default class map, check the <b>Use Class Default</b> check box.</li> </ol> <p>The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit <b>match any</b> statement that enables it to match all traffic.</p> <ol style="list-style-type: none"> <li>2. To use a previously created class map: <ol style="list-style-type: none"> <li>a. Clear the <b>Use Class Default</b> check box.</li> <li>b. In the Class Map Name field, select the class map to be used.</li> </ol> </li> </ol> |                                                                                                                                            |
| Match Condition | A match condition is used for this traffic policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                            |
|                 | Match Condition Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. |

Table 12-23 *HTTPS Server Load Balancing Policy Map Rules (continued)*

| Option        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | Match Condition Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Source Address | <p>A client source host IPv4 address and subnet mask, or IPv6 address and prefix length are used for the network traffic matching criteria.</p> <ol style="list-style-type: none"> <li>For the IP Address Type, select either <b>IPv4</b> or <b>IPv6</b> for the address type.</li> <li>In the Source IP Address field, enter the source IP address of the client in the format based on the address type (IPv4 or IPv6).</li> <li>For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.<br/>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</li> </ol> |
| Insert Before | <ol style="list-style-type: none"> <li>Indicate whether this rule is to precede another rule for this policy map: <ul style="list-style-type: none"> <li><b>N/A</b>—This option is not configured.</li> <li><b>False</b>—This rule is not to precede another rule in this policy map.</li> <li><b>True</b>—This rule is to precede another rule in this policy map.</li> </ul> </li> <li>If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.</li> </ol> |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with [Step 6](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.



**Note** If you selected the Insert Before option and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 6** In the Action table, click **Add** to add an entry or select an existing entry to modify, and then click **Edit**.

**Step 7** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

**Step 8** In the Action Type field, configure actions for this rule using the information in [Table 12-22](#).

**Table 12-24** Generic Server Load Balancing Policy Map Actions

| Action         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Drop           | <p>The ACE is to discard packets that match this policy map.</p> <p>In the Action Log field, specify whether the dropped packets are to be logged in the software by choosing one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>N/A</b>—This option is not configured.</li> <li>• <b>False</b>—Dropped packets are not to be logged in the software.</li> <li>• <b>True</b>—Dropped packets are to be logged in the software.</li> </ul>                                                                                                                                                                                                                                                                                   |
| Forward        | The ACE is to forward the traffic that match this policy map to its destination.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Reverse Sticky | <p>Reverse IP stickiness is an enhancement to regular stickiness and is used mainly in FWLB. It ensures that multiple distinct connections that are opened by hosts at both ends (client and server) are load-balanced and stuck to the same firewall. Reverse stickiness applies to such protocols as FTP, RTSP, SIP, and so on where there are separate control channels and data channels opened by the client and the server, respectively. For complete details about reverse stickiness, see the <i>Server Load-Balancing Guide, Cisco ACE Application Control Engine Appliance</i>.</p> <p>In the Sticky Group field, choose an existing IPv4 IP netmask or IPv6 prefix sticky group that you want to associate with reverse IP stickiness.</p> |

Table 12-24 Generic Server Load Balancing Policy Map Actions (continued)

| Action             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Farm        | <p>The ACE is to load balance client requests for content to a server farm.</p> <ol style="list-style-type: none"> <li>1. In the Server Farm field, select the server farm for this policy map action.</li> <li>2. In the Backup Server Farm field, select the backup server farm for this action.</li> <li>3. Check the Sticky Enabled check box to indicate that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky.</li> <li>4. Check the Aggregate State Enabled check box to indicate that the operational state of the backup server farm is taken into consideration when evaluating the state of the load-balancing class in a policy map. Clear this check box to indicate that the operational state of the backup server farm is not taken into consideration when evaluating the state of the load-balancing class in a policy map.</li> </ol> |
| Server Farm-NAT    | <p>The ACE is to apply dynamic NAT to traffic for this policy map.</p> <ol style="list-style-type: none"> <li>1. In the NAT Pool ID field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are integers from 1 to 2147483647. For information on configuring NAT pools, see <a href="#">Configuring VLAN Interface NAT Pools and Displaying NAT Utilization, page 10-32</a>.</li> <li>2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 to 4094.</li> <li>3. In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.</li> </ol>                                                                                                                                                                                                              |
| Set-IP-TOS         | <p>The ACE is to set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings.</p> <p>In the IP TOS Rewrite Value (Bytes) field, enter the IP DSCP value. Valid entries are integers from 0 to 255.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Sticky-Server Farm | <p>The ACE is to load balance client requests for content to a sticky server farm.</p> <p>In the Sticky Group field, select the sticky group to be used for requests that match this policy map. ACE displays all stick groups configured on the virtual context; however, only the following sticky types are applicable for a load balancing policy map: IP Netmask, IPv6 Prefix, and SSL. ACE displays an error message if you choose an incorrect sticky type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Step 9** Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to deploy your entries and to configure another action.

**Related Topics**

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for RADIUS Server Load Balancing

Use this procedure to configure the rules and actions for RADIUS traffic received by the ACE.

### Assumptions

- A RADIUS server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

### Procedure

- 
- |               |                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; <i>context</i> &gt; Expert &gt; Policy Maps</b> . The Policy Maps table appears.                        |
| <b>Step 2</b> | In the Policy Maps table, select the RADIUS server load balancing policy map you want to set rules and actions for. The Rule table appears.         |
| <b>Step 3</b> | In the Rule table, click <b>Add</b> to add a new rule, or select the rule you want to modify, and then click <b>Edit</b> . The Rule screen appears. |
| <b>Step 4</b> | In the Type field, configure rules using the information in <a href="#">Table 12-25</a> .                                                           |

Table 12-25 RADIUS Server Load Balancing Policy Map Rules

| Option          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>Specify a class map to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>To use the class-default class map, check the Use Class Default check box.<br/> <p>The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit <b>match any</b> statement that enables it to match all traffic.</p> </li> <li>To use a previously created class map: <ol style="list-style-type: none"> <li>Clear the Use Class Default check box.</li> <li>In the Class Map Name field, select the class map to be used.</li> </ol> </li> </ol>                                                                                                                                                                                                                                                                            |
| Match Condition | <p>Specify a match condition to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>In the Match Condition Type field, select the type of match condition to use for this policy map: <ul style="list-style-type: none"> <li>Calling Station ID—A unique identifier of the calling station is used to establish a match condition.<br/> <p>In the RADIUS Calling Station ID field, enter the calling station identifier to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use for matching string expressions.</p> </li> <li>User Name—A username is used to establish a match condition.<br/> <p>In the User Name field, enter the name to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use for matching string expressions.</p> </li> </ul> </li> </ol> |
| Insert Before   | <ol style="list-style-type: none"> <li>Indicate whether this rule is to precede another rule for this policy map. <ul style="list-style-type: none"> <li>N/A—This option is not configured.</li> <li>False—This rule is not to precede another rule in this policy map.</li> <li>True—This rule is to precede another rule in this policy map.</li> </ul> </li> <li>If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. To enter actions for this rule, continue with [Step 6](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to configure another rule.

**Note**

If you selected the Insert Before option and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 6** In the Action table, click **Add** to add an entry or select an existing entry to modify, and then click **Edit**.
- Step 7** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.
- Step 8** In the Action Type field, configure actions for this rule using the information in [Table 12-22](#).
- Step 9** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
  - Click **Next** to deploy your entries and to configure another action.

**Related Topics**

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for RTSP Server Load Balancing

Use this procedure to configure the rules and actions for RTSP traffic received by the ACE.

**Assumptions**

- An RTSP server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

**Procedure**

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the RTSP server load balancing policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
- Step 4** In the Type field, configure rules using the information in [Table 12-26](#).

Table 12-26 RTSP Server Load Balancing Policy Map Rules

| Option          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>Specify a class map to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>To use the class-default class map, check the Use Class Default check box.<br/> The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit <b>match any</b> statement that enables it to match all traffic.</li> <li>To use a previously created class map: <ol style="list-style-type: none"> <li>Clear the Use Class Default check box.</li> <li>In the Class Map Name field, select the class map to be used.</li> </ol> </li> </ol> |
| Match Condition | <p>Specify a match condition to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in <a href="#">Table 12-27</a>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Insert Before   | <ol style="list-style-type: none"> <li>Indicate whether this rule is to precede another rule for this policy map. <ul style="list-style-type: none"> <li>N/A—This option is not configured.</li> <li>False—This rule is not to precede another rule in this policy map.</li> <li>True—This rule is to precede another rule in this policy map.</li> </ul> </li> <li>If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 12-27** RTSP Policy Map Match Conditions

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RTSP Header     | <p>RTSP header information is used for matching criteria.</p> <ol style="list-style-type: none"> <li>In the Header Name field, specify the header to match in one of the following ways: <ul style="list-style-type: none"> <li>To specify an RTSP header that is not one of the standard RTSP headers, select the first radio button, then enter the RTSP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</li> <li>To specify a standard RTSP header, click the second radio button, then select an RTSP header from the list.</li> </ul> </li> <li>In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the RTSP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol> |
| RTSP URL        | <p>A URL or portion of a URL is used for match criteria.</p> <ol style="list-style-type: none"> <li>In the URL Expression field, enter a URL, or portion of a URL, to match. The ACE performs matching on whatever URL string appears after the RTSP method, regardless of whether the URL includes the host name. The ACE supports regular expressions for matching URL strings. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> <li>In the Method Expression field, enter the RTSP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can be either one of the standard RTSP method names (DESCRIBE, ANNOUNCE, GET_PARAMETER, OPTIONS, PAUSE, PLAY, RECORD, REDIRECT, SETUP, SET_PARAMETER, TEARDOWN) or a text string that must be matched exactly (for example, STINGRAY).</li> </ol>                                                                                                                                                                                                                     |
| Source Address  | <p>The source IP address is used for match criteria.</p> <ol style="list-style-type: none"> <li>For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.<br/><br/>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Step 5** In the Insert Before field, indicate whether this rule is to precede another rule for this policy map.

- N/A—This option is not configured.
- False—This rule is not to precede another rule in this policy map.
- True—This rule is to precede another rule in this policy map.

If you select True in the Insert Before field, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with [Step 7](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to add another rule.



**Note** If you selected the Insert Before option in [Step 5](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 7** In the Action table, click **Add** to add an entry or select an existing entry to modify, and then click **Edit**.
- Step 8** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.
- Step 9** In the Action Type field, configure actions for this rule using the information in [Table 12-22](#).
- Step 10** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
  - Click **Next** to deploy your entries and to configure another action.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for SIP Server Load Balancing

Use this procedure to configure the rules and actions for SIP traffic received by the ACE.

#### Assumptions

- A SIP server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

#### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the SIP server load balancing policy map you want to set rules and actions for. The Rule table appears.



- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
- Step 4** In the Type field, configure rules using the information in [Table 12-28](#).

**Table 12-28** SIP Server Load Balancing Policy Map Rules

| Option          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>Specify a class map to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>To use the class-default class map, check the Use Class Default check box.<br/>The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit <b>match any</b> statement that enables it to match all traffic.</li> <li>To use a previously created class map: <ol style="list-style-type: none"> <li>Clear the Use Class Default check box.</li> <li>In the Class Map Name field, select the class map to be used.</li> </ol> </li> </ol> |
| Match Condition | <p>Specify a match condition to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in <a href="#">Table 12-29</a>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Insert Before   | <ol style="list-style-type: none"> <li>Indicate whether this rule is to precede another rule for this policy map. <ul style="list-style-type: none"> <li>N/A—This option is not configured.</li> <li>False—This rule is not to precede another rule in this policy map.</li> <li>True—This rule is to precede another rule in this policy map.</li> </ul> </li> <li>If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 12-29 SIP Server Load Balancing Policy Map Match Conditions

| Match Condition | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIP Header      | <p>SIP header information is used for matching criteria.</p> <ol style="list-style-type: none"> <li>In the Header Name field, specify the header to match in one of the following ways: <ul style="list-style-type: none"> <li>To specify a SIP header that is not one of the standard SIP headers, select the first radio button, and then enter the SIP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.</li> <li>To specify a standard SIP header, click the second radio button, and then select an SIP header from the list.</li> </ul> </li> <li>In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the SIP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol> |
| Source Address  | <p>The source IP address is used for match criteria.</p> <p>The source IP address is used to establish a match condition.</p> <ol style="list-style-type: none"> <li>For the IP Address Type, select either IPv4 or IPv6 for the address type.</li> <li>In the Source IP Address field, enter the source IP address for this match condition in the format based on the address type (IPv4 or IPv6).</li> <li>For an IPv4 source address, in the Source Netmask field, select the subnet mask of the IP address.</li> </ol> <p>For an IPv6 source address, in the Source Prefix-length field, enter the prefix length for the address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears so you can enter actions for this rule. Continue with [Step 6](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to add another rule.



**Note** If you selected the Insert Before option in [Step 4](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

- Click the Rule tab to refresh the Rule table.
- In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 6** In the Action table, click **Add** to add an entry or select an existing entry to modify, and then click **Edit**.

**Step 7** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

**Step 8** In the Action Type field, configure actions for this rule using the information in [Table 12-22](#).

**Step 9** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to deploy your entries and to configure another action.

---

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for RDP Server Load Balancing

Use this procedure to configure the rules and actions for RDP traffic received by the ACE.

#### Assumptions

- An RDP server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

#### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the RDP server load balancing policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
- Step 4** In the Type field, confirm that Class Map is selected.
- Step 5** To use the class-default class map, check the Use Class Default check box.
- The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.
- Step 6** To use a previously created class map:
- a. Clear the Use Class Default check box.
  - b. In the Class Map Name field, select the class map to be used.

- Step 7** In the Insert Before field, indicate whether this rule is to precede another rule for this policy map.
- N/A—This option is not configured.
  - False—This rule is not to precede another rule in this policy map.
  - True—This rule is to precede another rule in this policy map.
- If you select True in the Insert Before field, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

- Step 8** Do the following:
- Click **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. To enter actions for this rule, continue with [Step 9](#).
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
  - Click **Next** to deploy your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 7](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 9** In the Action table, click **Add** to add an entry or select an existing entry to modify, and then click **Edit**.
- Step 10** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.
- Step 11** In the Action Type field, configure actions for this rule using the information in [Table 12-22](#).
- Step 12** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE.
  - Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
  - Click **Next** to deploy your entries and to configure another action.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection

Use this procedure to add rules and actions for Layer 7 HTTP deep packet inspection policy maps.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the Layer 7 deep packet inspection policy map that you want to set rules and actions for, and then select the Rule tab. You can select multiple policy maps (hold down the Shift key while selecting entries) and apply common rules and actions to them.
- Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.
- Step 4** In the Type field, select the type of rule to be used:
- **Class Map**—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions. Continue with [Step 5](#).
  - **Match Condition**—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions. Continue with [Step 7](#).
- Step 5** For class maps, check the Use Class Default check box to use the class-default class map, or clear the check box to use a previously created class map.
- Step 6** If you clear the Use Class Default check box:
- a. In the Class Map Name field, select the class map to be used.
  - b. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.
    - **N/A**—Indicates that this option is not configured.
    - **False**—Indicates that this rule is not to precede another rule in this policy map.
    - **True**—Indicates that this rule is to precede another rule in this policy map.
  - c. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 7** For match conditions:
- a. In the Match Condition Name field enter a name for the match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
  - b. In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See [Table 12-30](#) for information about these selections.

Table 12-30 HTTP Deep Packet Inspection Match Types

| Match Condition Type      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content                   | <p>Specific content contained within the HTTP entity-body is used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters.</li> <li>2. In the Content Offset (Bytes) field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 4000 bytes.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Content Length            | <p>The content parse length in an HTTP message is used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Content Length Operator field, select the operand to be used to compare content length: <ul style="list-style-type: none"> <li>– Equal To—Indicates that the content length must equal the number in the Content Length Value (Bytes) field.</li> <li>– Greater Than—Indicates that the content length must be greater than the number in the Content Length Value (Bytes) field.</li> <li>– Less Than—Indicates that the content length must be less than the number in the Content Length Value (Bytes) field.</li> <li>– Range—Indicates that the content length must be within the range specified in the Content Length Lower Value (Bytes) field and the Content Length Higher Value (Bytes) field.</li> </ul> </li> <li>2. Enter values to apply for content length comparison: <ul style="list-style-type: none"> <li>– If you select Equal To, Greater Than, or Less Than in the Content Length Operator field, the Content Length Value (Bytes) field appears. In the Content Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are integers from 0 to 4294967295.</li> <li>– If you select Range in the Content Length Operator field, the Content Length Lower Value (Bytes) and the Content Length Higher Value (Bytes) fields appear: <ol style="list-style-type: none"> <li>1. In the Content Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value (Bytes) field.</li> <li>2. In the Content Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value (Bytes) field.</li> </ol> </li> </ul> </li> </ol> |
| Content Type Verification | <p>Verifies the content MIME-type messages with the header MIME-type. This inline match command limits the MIME-types in HTTP messages allowed through the ACE appliance. It verifies that the header MIME-type value is in the internal list of supported MIME-types and the header MIME-type matches the actual content in the data or entity body portion of the message. If they do not match, the ACE appliance performs the specified Layer 7 policy map action.</p> <p><b>Note</b> Content Type Verification is only available as an inline match condition. Because this Layer 7 HTTP deep inspection match criteria cannot be combined with other match criteria, it appears as an inline match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 12-30 HTTP Deep Packet Inspection Match Types (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Header               | <p>The name and value in an HTTP header are used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header.</li> <li>2. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>3. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Header Length        | <p>The length of the header in the HTTP message is used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: <ul style="list-style-type: none"> <li>– Request—Indicates that HTTP header request messages are to be checked for header length.</li> <li>– Response—Indicates that HTTP header response messages are to be checked for header length.</li> </ul> </li> <li>2. In the Header Length Operator field, select the operand to be used to compare header length: <ul style="list-style-type: none"> <li>– Equal To—Indicates that the header length must equal the number in the Header Length Value (Bytes) field.</li> <li>– Greater Than—Indicates that the header length must be greater than the number in the Header Length Value (Bytes) field.</li> <li>– Less Than—Indicates that the header length must be less than the number in the Header Length Value (Bytes) field.</li> <li>– Range—Indicates that the header length must be within the range specified in the Header Length Lower Value (Bytes) field and the Header Length Higher Value (Bytes) field.</li> </ul> </li> <li>3. Enter values to apply for header length comparison: <ul style="list-style-type: none"> <li>– If you select Equal To, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value (Bytes) field appears. In the Header Length Value (Bytes) field, enter the number of bytes for comparison. Valid entries are integers from 0 to 255.</li> <li>– If you select Range in the Header Length Operator field, the Header Length Lower Value (Bytes) and the Header Length Higher Value (Bytes) fields appear: <ol style="list-style-type: none"> <li>1. In the Header Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value (Bytes) field.</li> <li>2. In the Header Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value (Bytes) field.</li> </ol> </li> </ul> </li> </ol> |

Table 12-30 HTTP Deep Packet Inspection Match Types (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Header MIME Type     | <p>Multipurpose Internet Mail Extension (MIME) message types are used for application inspection decisions.</p> <p>In the Header MIME Type field, select the MIME message type to be used for this match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Port Misuse          | <p>The misuse of port 80 (or any other port running HTTP) is used for application inspection decisions.</p> <p>Indicate the application category to be used for this match condition:</p> <ul style="list-style-type: none"> <li>IM—Indicates that instant messaging applications are to be used for this match condition.</li> <li>P2P—Indicates that peer-to-peer applications are to be used for this match condition.</li> <li>Tunneling—Indicates that tunneling applications are to be used for this match condition.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Request Method       | <p>The request method is used for application inspection decisions.</p> <p>By default, ACE appliances allow all request and extension methods. This option allows you to configure class maps that define application inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods.</p> <ol style="list-style-type: none"> <li>In the Request Method Type field, select the type of compliance to be used for application inspection decision: <ul style="list-style-type: none"> <li>Ext—Indicates that an HTTP extension method is to be used for application inspection decisions.</li> <li>RFC—Indicates that a request method defined in RFC 2616 is to be used for application inspection decisions.</li> </ul> <p>Depending on your selection, the Ext Request Method field or the RFC Request Method field appears.</p> </li> <li>In the Request Method field, select the specific request method to be used.</li> </ol> |
| Strict HTTP          | <p>Internal compliance checks are performed to verify that a message is compliant with the HTTP RFC standard, RFC 2616. If the HTTP message is not compliant, the ACE appliance performs the specified Layer 7 policy map action.</p> <p><b>Note</b> Strict HTTP is only available as an inline match condition. Because this Layer 7 HTTP deep inspection match criteria cannot be combined with other match criteria, it appears as an inline match condition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



Table 12-30 HTTP Deep Packet Inspection Match Types (continued)

| Match Condition Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transfer Encoding    | <p>An HTTP transfer-encoding type is used for application inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient.</p> <p>In the Transfer Encoding field, select the type of encoding that is to be checked:</p> <ul style="list-style-type: none"> <li>• Chunked—The message body is transferred as a series of chunks.</li> <li>• Compress—The encoding format that is produced by the UNIX file compression program compress.</li> <li>• Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951.</li> <li>• Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952.</li> <li>• Identity—The default (identity) encoding which does not require the use of transformation.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| URL                  | <p>URL names are used for application inspection decisions.</p> <p>In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| URL Length           | <p>URL length is used for application inspection decisions.</p> <ol style="list-style-type: none"> <li>1. In the URL Length Operator field, select the operand to be used to compare URL length: <ul style="list-style-type: none"> <li>– Equal To—Indicates that the URL length must equal the number in the URL Length Value (Bytes) field.</li> <li>– Greater Than—Indicates that the URL length must be greater than the number in the URL Length Value (Bytes) field.</li> <li>– Less Than—Indicates that the URL length must be less than the number in the URL Length Value (Bytes) field.</li> <li>– Range—Indicates that the URL length must be within the range specified in the URL Length Lower Value (Bytes) field and the URL Length Higher Value (Bytes) field.</li> </ul> </li> <li>2. Enter values to apply for URL length comparison: <ul style="list-style-type: none"> <li>– If you select Equal To, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value (Bytes) field appears. In the URL Length Value (Bytes) field, enter the value for comparison. Valid entries are from 1 to 65535 bytes.</li> <li>– If you select Range in the URL Length Operator field, the URL Length Lower Value (Bytes) and the URL Length Higher Value (Bytes) fields appear: <ol style="list-style-type: none"> <li>1. In the URL Length Lower Value (Bytes) field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value (Bytes) field.</li> <li>2. In the URL Length Higher Value (Bytes) field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value (Bytes) field.</li> </ol> </li> </ul> </li> </ol> |

- Step 8** In the Insert Before field, specify whether this rule is to precede another rule in this policy map:
- N/A—Indicates that this attribute is not set.
  - False—Indicates that this rule is not to precede another rule in the policy map.
  - True—Indicates that this rule is to precede another rule in the policy map.
- Step 9** If you set Insert Before to **True**, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 10** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with [Step 11](#).
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
  - Click **Next** to save your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 8](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 11** To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.
- Step 12** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- Step 13** In the Action Type field, select the action to be taken for this rule:
- Permit—Indicates that the specified HTTP traffic is to be allowed if it meets the specified HTTP deep packet inspection match criteria.
  - Reset—Indicates that the specified HTTP traffic is to be denied. A TCP reset message is sent to the client or server to close the connection.
- Step 14** Do the following:
- Click **Deploy Now** to deploy this configuration on the ACE appliance.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.
  - Click **Next** to configure another action for this policy map and rule.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection

File Transfer Protocol (FTP) inspection inspects FTP sessions for address translation in a message, dynamic opening of ports, and stateful tracking of request and response messages. Each specified FTP command must be acknowledged before the ACE allows a new command. Command filtering allows you to restrict specific commands by the ACE. When the ACE denies a command, it closes the connection.

The FTP command inspection process, as performed by the ACE:

- Prepares a dynamic secondary data connection. The channels are allocated in response to a file upload, a file download, or a directory listing event and must be prenegotiated. The port is negotiated through the PORT or PASV commands.
- Tracks the FTP command-response sequence. The ACE performs the command checks listed below. If you specify the FTP Strict field in a Layer 3 and Layer 4 policy map, the ACE tracks each FTP command and response sequence for the anomalous activity outlined below. The FTP Strict parameter is used in conjunction with a Layer 7 FTP policy map (nested within the Layer 3 and Layer 4 policy map) to deny certain FTP commands or to mask the server reply for SYST command.



### Note

The use of the FTP Strict parameter may affect FTP clients that do not comply with the RFC standards.

- Truncated command—Checks the number of commas in the PORT and PASV reply command against a fixed value of five. If the value is not five, the ACE assumes that the PORT command is truncated and issues a warning message and closes the TCP connection.
- Incorrect command—Checks the FTP command to verify if it ends with <CR><LF> characters, as required by RFC 959. If the FTP command does not end with those characters, the ACE closes the connection.
- Size of RETR and STOR commands—Checked the size of the RETR and STOR commands against a fixed constant of 256. If the size is greater, the ACE logs an error message and closes the connection.
- Command spoofing—Verifies that the PORT command is always sent from the client. If a PORT command is sent from the server, the ACE denies the TCP connection.
- Reply spoofing—Verifies that the PASV reply command (227) is always sent from the server. If a PASV reply command is sent from the client, the ACE denies the TCP connection. This denial prevents a security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- Invalid port negotiation—Checks the negotiated dynamic port value to verify that it is greater than 1024 (port numbers in the range from 2 to 1024 are reserved for well-known connections). If the negotiated port falls in this range, the ACE closes the TCP connection.
- Command pipelining—Checks the number of characters present after the port numbers in the PORT and PASV reply command against a constant value of 8. If the number of characters is greater than 8, the ACE closes the TCP connection.
- Translates embedded IP addresses in conjunction with NAT. FTP command inspection translates the IP address within the application payload. Refer to RFC 959 for background details.

Use this procedure to add rules and actions for Layer 7 FTP command inspection policy maps.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the Layer 7 FTP command inspection policy map you want to set rules and actions for, and then select the Rule tab. You can select multiple policy maps (hold down the Shift key while selecting entries) and apply common rules and actions to them.
- Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.
- Step 4** In the Type field, select the type of rule to be used:
- **Class Map**—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions.
  - **Match Condition**—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions.
- Step 5** For class maps, check the Use Class Default check box to use the class-default class map, or clear the check box to use a previously created class map.
- Step 6** If you clear the Use Class Default check box:
- a. In the Class Map Name field, select the class map to be used.
  - b. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.
    - N/A—Indicates that this option is not configured.
    - False—Indicates that this rule is not to precede another rule in this policy map.
    - True—Indicates that this rule is to precede another rule in this policy map.
  - c. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 7** For match conditions:
- a. In the Match Condition Name field enter a name for the match condition for this rule. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
  - b. In the Match Condition Type field, select Request Method Name as the match condition type for this rule.
  - c. In the Request Method Name field, select the FTP command to be inspected for this rule. [Table 12-13](#) describes the FTP commands that can be inspected.
- Step 8** In the Insert Before field, specify whether this rule is to precede another rule in this policy map:
- N/A—Indicates that this attribute is not set.
  - False—Indicates that this rule is not to precede another rule in the policy map.
  - True—Indicates that this rule is to precede another rule in the policy map.
- Step 9** If you set Insert Before to **True**, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

**Step 10** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with [Step 11](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Policy Maps table.
- Click **Next** to save your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 8](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 11** To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

**Step 12** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

**Step 13** In the Action Type field, specify the action to be taken for this rule:

- Deny—Indicates that the ACE appliance is to deny the specified FTP command when this rule is met.
- Mask Reply—Indicates that the ACE appliance is to mask the reply to the FTP **sys**t command by filtering sensitive information from the command output. The action applies to the FTP **sys**t command only.

**Step 14** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.
- Click **Next** to save your entries and to configure another action for this rule.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection

Use this procedure to configure the rules and actions for a SIP deep packet inspection policy map.

### Assumptions

- A SIP deep packet inspection policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
- Step 2** In the Policy Maps table, select the SIP deep packet inspection policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
- Step 4** In the Type field, configure rules using the information in [Table 12-31](#).

**Table 12-31** Layer 7 SIP Deep Packet Inspection Policy Map Rules

| Option          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class Map       | <p>Specify a class map to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>1. To use the class-default class map, check the Use Class Default check box.<br/><br/>The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit <b>match any</b> statement that enables it to match all traffic.</li> <li>2. To use a previously created class map: <ol style="list-style-type: none"> <li>a. Clear the Use Class Default check box.</li> <li>b. In the Class Map Name field, select the class map to be used.</li> </ol> </li> </ol> |
| Match Condition | <p>Specify a match condition to use for this traffic policy:</p> <ol style="list-style-type: none"> <li>1. In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>2. In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in <a href="#">Table 5-7</a>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Insert Before   | <ol style="list-style-type: none"> <li>1. Indicate whether this rule is to precede another rule for this policy map. <ul style="list-style-type: none"> <li>– N/A—This option is not configured.</li> <li>– False—This rule is not to precede another rule in this policy map.</li> <li>– True—This rule is to precede another rule in this policy map.</li> </ul> </li> <li>2. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Step 5** Do the following:

- Click **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with [Step 6](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to add another rule.



**Note** If you selected the Insert Before option and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 6** In the Action table, click **Add** to add an entry or select an existing entry to modify, and then click **Edit**.

**Step 7** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

**Step 8** In the Action Type field, select the action to be taken for this rule:

- Drop—The SIP traffic is to be dropped if it meets the specified match criteria.
- Permit—The SIP traffic is to be allowed if it meets the specified match criteria.
- Reset—The SIP traffic is to be denied if it meets the specified match criteria. A TCP reset message is sent to the client or server to close the connection.

**Step 9** In the Action Log field, specify whether the action taken is to be logged.

- N/A—This option is not configured.
- False—Dropped packets are not to be logged in the software.
- True—Dropped packets are to be logged in the software.

**Step 10** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to deploy your entries and to configure another action.

---

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection

Use this procedure to configure the rules and actions for a Skinny Client Control Protocol (SCCP) deep packet inspection policy map.

### Assumptions

- A Skinny deep packet inspection policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
  - Step 2** In the Policy Maps table, select the Skinny deep packet inspection policy map you want to set rules and actions for. The Rule table appears.
  - Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, and then click **Edit**. The Rule screen appears.
  - Step 4** In the Type field, confirm that Match Condition is selected.
  - Step 5** In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
  - Step 6** In the Match Condition Type field, confirm that Message ID is selected.
  - Step 7** In the Message ID Operator field, indicate whether the match criteria is for a single message identifier or for a range of message identifiers:
    - Equal To—A single message identifier is used for this match condition.  
In the Message ID Value field, enter the numerical identifier of a SCCP message. Valid entries are integers from 0 to 65535.
    - Range—A range of message identifiers is used for this match condition.
      - a.** In the Message ID Low Range Value field, enter the lowest numerical identifier of a range of SCCP messages. Valid entries are integers from 0 to 65535.
      - b.** In the Message ID High Range Value field, enter the highest numerical identifier of a range of SCCP messages. Valid entries are integers from 0 to 65535, and the value in this field must equal or be greater than the value in the Message ID Low Range Value field.
  - Step 8** In the Insert Before field, indicate whether this rule is to precede another rule in this policy map:
    - N/A—This option is not configured.
    - False—This rule is not to precede another rule in this policy map.
    - True—This rule is to precede another rule in this policy map.
  - Step 9** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.



**Step 10** Do the following:

- Click **Deploy Now** to deploy the configuration on the ACE. The screen refreshes and the Action table appears. To define the actions for this rule, continue with [Step 11](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to deploy your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 8](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 11** In Action table, click **Add** to add a new action, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

**Step 12** In the ID field, accept the automatically incremented entry or assign a unique identifier for this action.

**Step 13** In the Action Type field, confirm that Reset is selected.

**Step 14** In the Action Log field, specify whether the action taken is to be logged.

- N/A—This option is not configured.
- False—Dropped packets are not to be logged in the software.
- True—Dropped packets are to be logged in the software.

**Step 15** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- Click **Next** to deploy your entries and to configure another action.

---

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization

Use this procedure to add rules and actions for Layer 7 HTTP optimization policy maps.

### Assumptions

- An HTTP optimization action list has been configured. See [Configuring an HTTP Optimization Action List, page 13-3](#) for more information.
- A class map has been defined if you are not using the class-default class map. See [Configuring Virtual Context Class Maps, page 12-8](#) for more information.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > context > Expert > Policy Maps**. The Policy Maps table appears.
  - Step 2** In the Policy Maps table, select the Layer 7 HTTP optimization policy map you want to set rules and actions for, and then select the Rule tab. You can select multiple policy maps (hold down the Shift key while selecting entries) and apply common rules and actions to them.
  - Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, and then **Edit** to modify it. The Rule configuration screen appears.
  - Step 4** In the Type field, select the type of rule to be used:
    - **Class Map**—Indicates that the ACE appliance is to use an existing class map that identifies the rules and corresponding actions.
    - **Match Condition**—Indicates that the ACE appliance is to use a set of conditions to identify the rules and corresponding actions.
  - Step 5** For class maps, check the Use Class Default check box to use the class-default class map, or clear the check box to use a previously created class map.
  - Step 6** If you clear the Use Class Default check box:
    - a. In the Class Map Name field, select the class map to be used.
    - b. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.
      - **N/A**—Indicates that this option is not configured.
      - **False**—Indicates that this rule is not to precede another rule in this policy map.
      - **True**—Indicates that this rule is to precede another rule in this policy map.
    - c. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
  - Step 7** For match conditions:
    - a. In the Match Condition Name field, enter a name for the match condition for this rule. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
    - b. In the Match Condition Type field, select the type of match condition to use and configure condition-specific options as described in [Table 12-32](#).

Table 12-32 Layer 7 HTTP Optimization Match Condition Types

| Match Condition Type | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cookie               | <p>Indicates that an HTTP cookie is to be used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters.</li> <li>3. In the Secondary Cookie check box, do one of the following: <ul style="list-style-type: none"> <li>– Clear the check box to indicate that the cookie being defined is a primary cookie.</li> <li>– Check the check box to indicate that the cookie being defined is a secondary cookie. You can specify the delimiters for cookies in a URL string by using an HTTP parameter map (see the “<a href="#">Configuring HTTP Parameter Maps</a>” section on page 8-2).</li> </ul> </li> </ol>                                                                 |
| Header               | <p>Indicates that an HTTP header is to be used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header.</li> <li>2. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.</li> <li>3. In the Header Value (Bytes) field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE appliance supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</li> </ol> |
| HTTP URL             | <p>Indicates that a portion of an HTTP URL is to be used to establish a match condition.</p> <ol style="list-style-type: none"> <li>1. In the URL Expression field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.</li> <li>2. In the Method Expression field, enter the HTTP method to match. Valid entries are method names entered as unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can enter either one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).</li> </ol>                                                                                                                        |

**Step 8** In the Insert Before field, specify whether this rule is to precede another rule in this policy map:

- N/A—Indicates that this attribute is not set.
- False—Indicates that this rule is not to precede another rule in the policy map.
- True—Indicates that this rule is to precede another rule in the policy map.

If you set Insert Before to **True**, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

**Step 9** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The Action table appears below the Rule table. To define actions for this rule, continue with [Step 10](#).
- Click **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- Click **Next** to save your entries and to configure another rule.



**Note** If you selected the Insert Before option in [Step 8](#) and specified **True**, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

**Step 10** To add an action for this rule, click **Add** in the Action table, or select an existing action, and then click **Edit** to modify it. The Action configuration screen appears.

**Step 11** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

**Step 12** In the Action Type field, select Action-list to indicate that an HTTP optimization action list is to be employed when the match criteria are met.

**Step 13** In the Action List field, select the HTTP optimization action list to apply to this policy map and rule. If necessary, click **Add** to add a new HTTP optimization action list, or select an existing action list, and then click **Edit** to modify it.

**Step 14** In the Optimization Parameter Map field, select the optimization parameter map to apply to this policy map and rule.

**Step 15** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Action table.
- Click **Next** to save your entries and to configure another action for this rule.

#### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Rules and Actions for Policy Maps, page 12-36](#)

## Special Characters for Matching String Expressions

Table 12-33 identifies the special characters that can be used in matching string expressions. Use parenthesized expressions for dynamic replacement using %1 and %2 in the replacement pattern.



### Note

When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter `www[.]xyz[.]com` instead of `www.xyz.com`). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

**Table 12-33** Special Characters for Matching String Expressions

| Convention    | Description                                                                         |
|---------------|-------------------------------------------------------------------------------------|
| .             | One of any character.                                                               |
| .*            | Zero or more of any character.                                                      |
| \.            | Period (escaped).                                                                   |
| \xhh          | Non-printable character.                                                            |
| [charset]     | Match any single character from the range.                                          |
| [^charset]    | Do not match any character in the range. All other characters represent themselves. |
| ()            | Expression grouping.                                                                |
| expr1   expr2 | OR of expressions.                                                                  |
| (expr)*       | 0 or more of expression.                                                            |
| (expr)+       | 1 or more of expression.                                                            |
| .\a           | Alert (ASCII 7).                                                                    |
| .\b           | Backspace (ASCII 8).                                                                |
| .\f           | Form-feed (ASCII 12).                                                               |
| .\n           | New line (ASCII 10).                                                                |
| .\r           | Carriage return (ASCII 13).                                                         |
| .\t           | Tab (ASCII 9).                                                                      |
| .\v           | Vertical tab (ASCII 11).                                                            |
| .\0           | Null (ASCII 0).                                                                     |
| .\            | Backslash.                                                                          |
| .\x##         | Any ASCII character as specified in two-digit hexadecimal notation.                 |

### Related Topics

- [Configuring Traffic Policies, page 12-1](#)
- [Configuring Virtual Context Class Maps, page 12-8](#)
- [Configuring Virtual Context Policy Maps, page 12-34](#)
- [Configuring Real Servers, page 6-5](#)

- [Configuring Server Farms, page 6-18](#)
- [Configuring Sticky Groups, page 7-11](#)

## Configuring Actions Lists

An action list is a named group of actions that you associate with a Layer 7 policy map. The ACE supports the following types action lists:

- An HTTP optimization action list groups a series of individual application acceleration and optimization operations that you want the ACE to perform. The HTTP optimization action list is associated with a Layer 7 HTTP optimization policy map (see the [“Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization” section on page 12-86](#)).
- An HTTP header modify action list performs the following operations:
  - Groups a series of individual functions to insert, rewrite, or delete HTTP headers.
  - Configures the SSL URL rewrite function.
  - Inserts SSL session parameters, client certificate fields, and server certificate fields into the HTTP requests that the ACE receives over the connection.

The HTTP header action list is associated with a Layer 7 server load-balancing policy map (see the [“Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic” section on page 12-46](#)).

[Table 12-34](#) lists the action lists that you can configure using the ACE.

**Table 12-34**      *Action Lists*

| Action List                    | Topic                                                                     |
|--------------------------------|---------------------------------------------------------------------------|
| Optimization Action List       | <a href="#">Configuring an HTTP Optimization Action List, page 13-3</a>   |
| HTTP Header Modify Action List | <a href="#">Configuring an HTTP Header Modify Action List, page 12-90</a> |

## Configuring an HTTP Header Modify Action List

An HTTP header modify action list groups a series of individual functions to insert, rewrite, or delete HTTP headers. It can also be used to configure the SSL URL rewrite function.

This procedure includes the following topics:

- [Configuring HTTP Header Insertion, Deletion, and Rewrite, page 12-91](#)
- [Configuring SSL URL Rewrite, page 12-94](#)
- [Configuring SSL Header Insertion, page 12-96](#)

## Configuring HTTP Header Insertion, Deletion, and Rewrite

Use this procedure to configure an HTTP header modify action list that inserts, rewrites, or deletes HTTP headers.

### Procedure

- 
- Step 1** Choose **Config > Virtual Contexts > *context* > Expert > Action Lists > HTTP Header Modify Action Lists**.
- The HTTP Header Modify Action List table appears.
- Step 2** Do one of the following:
- To edit an existing action list, choose the action list and click the **Edit** icon. The Edit HTTP Header Modify Action List window appears.
  - To create a new action list, do the following:
    - a. Click the **Add** icon. The New HTTP Header Modify Action List window appears.
    - b. In the Action List Name field, enter a unique name for the HTTP header modify action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
    - c. Click **Deploy Now**. The Edit HTTP Header Modify Action List window appears.
- Step 3** (Optional) To rewrite the URL pathname in HTTP requests, do the following:
- a. From the URL Expression field, enter the regular expression of the URL in the incoming request to match.
  - b. From the Replace field, enter the replacement URL string. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can also use the following dynamic replacement strings:
    - **%is**—Inserts the source IP address in the HTTP header
    - **%id**—Inserts the destination IP address in the HTTP header
    - **%ps**—Inserts the source port in the HTTP header
    - **%pd**—Inserts the destination port in the HTTP header
    - **%u**—Inserts the URL path string from the request
    - **%h**—Inserts the hostname from the request host header
- Step 4** (Optional) Content Rewrite Response String provides the capability to rewrite configured regex patterns in the HTTP response:
- a. The HTTP Content Rewrite feature provides the capability on the ACE module to re-write configured HTTP content in the HTTP response data.
  - b. The HTTP content ‘Rewrite response replace’ feature provides the capability on the ACE module to replace configured HTTP content in the HTTP response data.
- Step 5** Select the Header Action tab. The Header Action table appears.
- Step 6** Click **Add** to add a new entry to the Header Action table. The Header Action configuration screen appears. Enter the required information as shown in [Table 12-35](#).

**Table 12-35**      *Header Action Configuration Screen Fields*

| Header Action Field | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operator            | <p>Select the HTTP header modify action the ACE appliance is to take in an HTTP request from a client, a response from a server, or both:</p> <ul style="list-style-type: none"><li>• Delete—Deletes an HTTP header in a request from a client, in a response from a server, or both.</li><li>• Insert—Insert a header name and value in an HTTP request from a client, a response from a server, or both. When the ACE uses Network Address Translation (NAT) to translate the source IP address of a client to a VIP, servers need a way to identify that client for the TCP and IP return traffic. To identify a client whose source IP address has been translated using NAT, you can instruct the ACE to insert a generic header and string value of your choice in the client HTTP request.</li><li>• Rewrite—Rewrite an HTTP header in request packets from a client, response packets from a server, or both.</li></ul> |



Table 12-35 Header Action Configuration Screen Fields (continued)

| Header Action Field | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Direction           | <p>Select the HTTP header modify action the ACE appliance is to take with respect to the selected operator (Insert, Delete, or Rewrite):</p> <p>Insert:</p> <ul style="list-style-type: none"> <li>Both—Specifies that the ACE insert an HTTP header in both HTTP request packets and response packets.</li> <li>Request—Specifies that the ACE insert an HTTP header only in HTTP request packets from clients.</li> <li>Response—Specifies that the ACE insert an HTTP header only in HTTP response packets from servers.</li> </ul> <p>Delete:</p> <ul style="list-style-type: none"> <li>Both—Specifies that the ACE delete the header in both HTTP request packets and response packets.</li> <li>Request—Specifies that the ACE delete the header only in HTTP request packets from clients.</li> <li>Response—Specifies that the ACE delete the header only in HTTP response packets from servers.</li> </ul> <p>Rewrite:</p> <ul style="list-style-type: none"> <li>Both—Specifies that the ACE rewrite an HTTP header string in both HTTP request packets and response packets.</li> <li>Request—Specifies that the ACE rewrite an HTTP header string only in HTTP request packets from clients.</li> <li>Response—Specifies that the ACE rewrite an HTTP header string only in HTTP response packets from servers.</li> </ul> |
| Header Name         | Identifier of an HTTP header. Enter an unquoted text string with a maximum of 255 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Header Value        | <p>Specifies the value of the HTTP header that you want to insert or replace in request packets, response packets, or both. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can also use the following dynamic replacement strings:</p> <ul style="list-style-type: none"> <li><b>%is</b>—Inserts the source IP address in the HTTP header</li> <li><b>%id</b>—Inserts the destination IP address in the HTTP header</li> <li><b>%ps</b>—Inserts the source port in the HTTP header</li> <li><b>%pd</b>—Inserts the destination port in the HTTP header</li> </ul> <p>The ACE appliance supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</p>                                                                                                                                                                                                                                                                                                                                                                                                              |
| Replace             | Specifies the pattern string that you want to substitute for the header value regular expression. For dynamic replacement of the first and second parenthesized expressions from the header value, use %1 and %2, respectively.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Step 7** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to save your entries.

---

#### Related Topics

- [Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46, Table 12-20](#)

## Configuring SSL URL Rewrite



#### Note

The SSL URL rewrite feature does not apply to the ACE NPE software image (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

When a client sends encrypted traffic to the ACE in an SSL termination configuration, the ACE terminates the SSL traffic and then sends clear text to the server. Because the server is unaware of the encrypted traffic flowing between the client and the ACE, the server may return to the client a URL in the Location header of HTTP redirect responses (301: Moved Permanently or 302: Found) in the form <http://www.cisco.com> instead of <https://www.cisco.com>. In this case, the client makes a request to the unencrypted insecure URL, even though the original request was for a secure URL. Because the client connection changes to HTTP, the requested data may not be available from the server using a clear text connection.

To solve this problem, the ACE provides SSLURL rewrite, which changes the redirect URL from <http://> to <https://> in the Location response header from the server before sending the response to the client. By using URL rewrite, you can avoid nonsecure HTTP redirects. All client connections to the web server will be SSL, ensuring the secure delivery of HTTPS content back to the client. The ACE uses regular expression matching to determine whether the URL needs rewriting. If a Location response header matches the specified regular expression, the ACE rewrites the URL. In addition, the ACE provides parameters to add or change the SSL and the clear port numbers.

Use this procedure to configure an HTTP header modify action list that performs SSL URL rewrite.

#### Procedure

- 
- |               |                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Action Lists &gt; HTTP Header Modify Action Lists</b> . The HTTP Header Modify Action List table appears.                         |
| <b>Step 2</b> | Click <b>Add</b> to add a new HTTP header modify action list, or select an existing action list, and then click <b>Edit</b> to modify it.                                                              |
| <b>Step 3</b> | For a new action list, in the Action List Name field enter a unique name for the HTTP header modify action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters. |
| <b>Step 4</b> | Select the <b>SSL Action</b> tab. The SSL Action table appears.                                                                                                                                        |
| <b>Step 5</b> | Click <b>Add</b> to add a new entry to the SSL Action table. The SSL Action configuration screen appears. Enter the required information as shown in <a href="#">Table 12-36</a> .                     |

Table 12-36 SSL Action Configuration Screen Fields

| Header Action Field | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL Expression      | <p>Specifies the rewriting of the URL in the Location response header based on a URL regular expression match. If the URL in the Location header matches the URL regular expression string that you specify, the ACE rewrites the URL from http:// to https:// and rewrites the port number. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. Alternatively, you can enter a text string with spaces if you enclose the entire string in quotation marks (“”).</p> <p>The location regex that you enter must be a pure URL (for example, www\.cisco\.com) with no port or path designations. To match a port, use the SSL Port and Clear Port parameters. If you need to match a path, use the HTTP header rewrite feature to rewrite the string. For information about the HTTP header rewrite feature, see the <a href="#">“Configuring HTTP Header Insertion, Deletion, and Rewrite”</a> section on page 12-91.</p> <p>The ACE appliance supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See <a href="#">Table 12-33</a> for a list of the supported characters that you can use in regular expressions.</p> |
| SSL Port            | Specifies the SSL port number from which the ACE translates a clear port number before sending the server redirect response to the client. Enter an integer from 1 to 65535. The default is 443.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Clear Port          | Specifies the clear port number to which the ACE translates the SSL port number before sending a server redirect response to the client. Enter an integer from 1 to 65535. The default is 80.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Step 6** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to save your entries.

**Related Topics**

- [Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46, Table 12-20](#)

## Configuring SSL Header Insertion



### Note

The SSL Header Insertion feature does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).

You can configure an HTTP header modify action list that performs SSL header insertion.

When a client sends encrypted traffic to the ACE in an SSL termination configuration, the ACE terminates the SSL traffic and then sends clear text to the server, which is unaware of the encrypted traffic flowing between the client and the ACE. Using an action list associated with a Layer 7 HTTP load-balancing policy map, you can instruct the ACE to perform SSL HTTP header insertion. The ACE provides the server with the following SSL session information by inserting HTTP headers into the HTTP requests that it receives over the connection:

- Session Parameters—SSL session parameters that the ACE and client negotiate during the SSL handshake.
- Server Certificate Fields—Information regarding the SSL server certificate that resides on the ACE.
- Client Certificate Fields—Information regarding the SSL client certificate that the ACE retrieves from the client when you configure the ACE to perform client authentication.



### Note

To prevent HTTP header spoofing, the ACE deletes any incoming HTTP headers that match one of the headers that it is going to insert into the HTTP request.

By default, the ACE inserts the SSL header information into the first HTTP request only that it receives over the connection. When the ACE and client need to renegotiate their connection, the ACE updates the HTTP header information that it send to the server to reflect the new session parameters. You can also instruct the ACE to insert the session information into every HTTP request that it receives over the connection by creating an HTTP parameter map with either the **Header Modify Per-Request** or **HTTP Persistence Rebalance** options enabled (see the [“Configuring HTTP Parameter Maps”](#) section on page 8-2).



### Note

The maximum amount of data that the ACE can insert is 512 bytes. The ACE truncates the data if it exceeds this limit.

### Procedure

- Step 1** Choose **Config > Virtual Contexts > context > Expert > HTTP Header Modify Action Lists**.  
The HTTP Header Modify Action Lists table appears.
- Step 2** In the HTTP Header Modify Action Lists table, do one of the following:
  - To add a new action list, click **Add**. In the Action List Name field, enter a unique name for the action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters. Click **Deploy Now** when completed to save the configuration and display the editing tabs.
  - To edit an existing action list, choose the action list and click **Edit** to display the editing tabs.
- Step 3** Click the **SSL Header Insert** tab.  
The SSL Header Insert table appears.
- Step 4** In the SSL Header Insert table, click **Add** to add a new entry to the SSL Header Insert table.

The SSL Header Insert configuration window appears. Enter the required information as shown in [Table 12-37](#).

**Table 12-37** *SSL Header Insert Configuration Window Fields*

| Header Action Field | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Request             | <p>Select the type of SSL header information to insert into the HTTP request:</p> <ul style="list-style-type: none"> <li>• Client-Certificate—Information about the client certificate that the ACE retrieves from the client.</li> <li>• Server-Certificate—Information about the server certificate that resides on the ACE.</li> <li>• Session—Information about the session parameters that the ACE and client negotiated during the SSL handshake.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Algorithm           | <p>This field appears only when the Request field is set to either Client-Certificate or Server-Certificate. Select the following certificate field information to insert into the HTTP request:</p> <ul style="list-style-type: none"> <li>• Authority-Key-Id—X.509 authority key identifier.</li> <li>• Basic-Constraints—X.509 basic constraints.</li> <li>• Certificate-Version—X.509 certificate version.</li> <li>• Data-Signature-Algorithm—X.509 hashing and encryption method.</li> <li>• Fingerprint-SHA1—SHA1 hash of the certificate.</li> <li>• Issuer—X.509 certificate issuer's distinguished name.</li> <li>• Issuer-CN—X.509 certificate issuer's common name.</li> <li>• Not-After—Date after which the certificate is not valid.</li> <li>• Not-Before—Date before which the certificate is not valid.</li> <li>• Public-Key-Algorithm—Algorithm used for the public key.</li> <li>• RSA-Exponent—Public RSA exponent.</li> <li>• RSA-Modulus—RSA algorithm modulus.</li> <li>• RSA-Modulus-Size—Size of the RSA public key.</li> <li>• Serial-Number—Certificate serial number.</li> <li>• Signature—Certificate signature.</li> <li>• Signature-Algorithm—Certificate signature algorithm.</li> <li>• Subject—X.509 subject's distinguished name.</li> <li>• Subject-CN—X.509 subject's common name.</li> <li>• Subject-Key-Id—X.509 subject key identifier.</li> </ul> <p>For more information, see the <i>SSL Guide, Cisco ACE Application Control Engine</i>.</p> |

Table 12-37 SSL Header Insert Configuration Window Fields (continued)

| Header Action Field | Description / Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CipherKey           | <p>This field appears only when the Request field is set to Session. Select the following session parameters to insert into the HTTP request:</p> <ul style="list-style-type: none"> <li>• Cipher-Key-Size—Symmetric cipher key size.</li> <li>• Cipher-Name—Symmetric cipher suite name.</li> <li>• Cipher-Use-Size—Symmetric cipher use size.</li> <li>• Id—SSL Session ID. The default is 0.</li> <li>• Protocol-Version—Version of SSL or TLS.</li> <li>• Step-Up—Use of SGC or StepUp cryptography to increase the level of security by using 128-bit encryption.</li> <li>• Verify-Result—SSL session verify result. Possible values are as follows: <ul style="list-style-type: none"> <li>– ok—The SSL session is established.</li> <li>– certificate is not yet valid—The client certificate is not yet valid.</li> <li>– certificate is expired—The client certificate has expired.</li> <li>– bad key size—The client certificate has a bad key size.</li> <li>– invalid not before field—The client certificate notBefore field is in an unrecognized format.</li> <li>– invalid not after field—The client certificate notAfter field is in an unrecognized format.</li> <li>– certificate has unknown issuer—The client certificate issuer is unknown.</li> <li>– certificate has bad signature—The client certificate contains a bad signature.</li> <li>– certificate has bad leaf signature—The client certificate contains a bad leaf signature.</li> <li>– unable to decode issuer public key—The ACE is unable to decode the issuer public key.</li> <li>– unsupported certificate—The client certificate is not supported.</li> <li>– certificate revoked—The client certificate has been revoked.</li> <li>– internal error—An internal error exists.</li> </ul> </li> </ul> <p>For more information, see the <i>SSL Guide, Cisco ACE Application Control Engine</i>.</p> |
| Value               | <p>This field appears only when the Request field is set to either Client-Certificate or Server-Certificate. Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• N/A—Specifies that the selected algorithm or cipher key is inserted without adding a prefix to it or renaming it.</li> <li>• Prefix—Enables you to specify a prefix string to place before the specified certificate or session field name. For example, if you specify the prefix Acme-SSL for the SSL session field name Cipher-Name, then the field name becomes Acme-SSL-Session-Cipher-Name.</li> <li>• Rename—Enables you to specify a new name for the specified certificate or session field name.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Prefix              | <p>This field appears only when the Value field is set to Prefix. Enter a quoted text string to place before the specified certificate or session field name. The maximum combined number of prefix string and field name characters that the ACE permits is 32.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Rename              | <p>This field appears only when the Value field is set to Rename. Enter a new name to the specified certificate or session field name. The name must be an unquoted text string with no spaces. The maximum number of field name string characters that the ACE permits is 32.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Step 5** Repeat Step 4 for each certificate field or session parameter that you want the ACE to insert.

**Step 6** Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE and save your entries to the running-configuration and startup-configuration files.
  - Click **OK** to save your entries. This option appears for configuration building blocks.
  - Click **Cancel** to exit this procedure without saving your entries.
  - Click **Next** to deploy your entries and to add another entry to the SSL Header Insert table.
- 

#### Related Topics

- [Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 12-65, Table 12-20](#)







# CHAPTER 13

## Configuring Application Acceleration and Optimization

---

This chapter describes how to configure application acceleration and optimization. With application acceleration and optimization features, you can configure application delivery and application acceleration options that increase productivity and efficiency. The application acceleration features optimize network performance and improve access to critical business information. This capability accelerates the performance of Web applications, including customer relationship management, portals, and online collaboration by up to 10 times.



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

This section includes:

- [Optimization Overview, page 13-2](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)
- [Configuring an HTTP Optimization Action List, page 13-3](#)
- [Configuring Optimization Parameter Maps, page 13-6](#)
- [Configuring Traffic Policies for HTTP Optimization, page 13-6](#)
- [Enabling HTTP Optimization Using Virtual Servers, page 13-9](#)
- [Configuring Global Application Acceleration and Optimization, page 13-9](#)



### Note

Application acceleration performance on the ACE is 50 to 100 Mbps throughput. With typical page sizes and browser usage patterns, this equates to roughly 1,000 concurrent connections. Subsequent connections bypass the application acceleration engine. This limitation applies only to traffic that is explicitly configured to receive application acceleration processing (for example, FlashForward, Delta Optimization). Traffic that is not configured to receive application acceleration processing is not subject to these limitations. Also, because the ACE HTTP compression is implemented separately in hardware, it is not subject to these limitations. For example, if you have a mix of application-accelerated and

non-application-accelerated traffic, the former is limited; the latter is not. If you have 50 Mbps of application-accelerated traffic, the ACE can still deliver up to 1.9 Gbps throughput for the non-application-accelerated traffic.

---

## Optimization Overview

The application acceleration functions of the ACE appliance apply several optimization technologies to accelerate application performance. This functionality enables enterprises to optimize network performance and improve access to critical business information.

The ACE appliance provides the following application acceleration and optimization functionality:

- Delta optimization eliminates redundant traffic on the network by computing and transmitting only the changes that occur in a Web page between successive downloads of the same page or similar pages.
- FlashForward object acceleration technology eliminates network delays associated with embedded cacheable Web objects such as images, style sheets, and JavaScript files by placing the responsibility for validating object freshness on the ACE appliance, rather than on the client, making the client more efficient.
- Just-in-time object acceleration enables acceleration of non-cacheable embedded objects, resulting in improved application response time by eliminating the need for clients to download these objects on each request.
- Adaptive dynamic caching accelerates enterprise application performance and improves server system scalability by enabling the ACE appliance itself to fulfill requests for dynamic content, which offloads application servers and databases.

Refer to [Configuring Application Acceleration and Optimization, page 13-1](#) or the *Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance* for more information about application acceleration and optimization.

### Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)
- [Configuring Traffic Policies for HTTP Optimization, page 13-6](#)
- [Configuring Global Application Acceleration and Optimization, page 13-9](#)

## Optimization Traffic Policies and Typical Configuration Flow

To define the different optimization and application acceleration functions that you want the ACE to perform, you must configure at least one each of the following:

- HTTP optimization action list—This action list specifies the actions that the ACE is to perform for application acceleration and optimization. You can configure action lists when configuring a virtual server, or as a separate procedure. See:
  - [Configuring Application Acceleration and Optimization, page 13-1](#)
  - [Configuring an HTTP Optimization Action List, page 13-3.](#)

- Layer 7 server load-balancing class map—This class map identifies the Layer 7 server load-balancing match criteria to apply to incoming traffic, such as URL, HTTP cookie, HTTP header, or source IP address. See [Configuring Virtual Context Class Maps, page 12-8](#)
- Layer 7 HTTP optimization policy map—This policy map applies the HTTP optimization action list and optionally an optimization parameter map to Layer 7 HTTP traffic. See [Configuring Virtual Context Policy Maps, page 12-34](#).
- Layer 3 and Layer 4 class map—By using match criteria, this class map identifies the network traffic that can pass through the ACE appliance. The match criteria includes the VIP address for the network traffic. The ACE appliance uses these Layer 3 and Layer 4 traffic classes to perform server load balancing. See [Configuring Virtual Context Class Maps, page 12-8](#).
- Layer 3 and Layer 4 policy map—This policy map associates server load-balancing actions and HTTP optimization action lists with the VIP. See [Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic, page 12-45](#) and [Configuring Traffic Policies for HTTP Optimization, page 13-6](#).
- Layer 7 server load-balancing policy map—This policy map specifies the server load-balancing actions that the ACE appliance is to perform. See [Configuring Virtual Context Policy Maps, page 12-34](#).

You can also configure:

- Optimization parameter maps—Optimization parameter maps allow you to configure specific options for action list items. You can configure optimization parameter maps when configuring a virtual server or as a separate procedure.

When you configure a parameter map with an action list for a class map, the ACE appliance validates the action list and parameter map configurations before deploying them.

See:

- [Configuring Application Acceleration and Optimization, page 5-57](#)
- [Configuring Optimization Parameter Maps, page 8-11](#)
- Global application acceleration and optimization options—The acceleration and optimization options allow you to apply specific acceleration and optimization features for logging and debugging on a global level on the ACE appliance. See [Configuring Global Application Acceleration and Optimization, page 13-9](#).

#### Related Topics

- [Configuring Traffic Policies for HTTP Optimization, page 13-6](#)
- [Optimization Overview, page 13-2](#)

## Configuring an HTTP Optimization Action List

An HTTP optimization action list groups a series of individual application acceleration and optimization operations that you want the ACE to perform.

Use this procedure to configure an HTTP optimization action list.



#### Tip

You can also configure HTTP optimization action lists when configuring a virtual server. For more information, see [Configuring Application Acceleration and Optimization, page 5-57](#).

**Procedure**

- Step 1** Select **Config > Virtual Contexts > context > Expert > Action Lists > Optimization Action Lists**. The Optimization Action List table appears.
- Step 2** Click **Add** to add a new optimization action list, or select an existing action list, and then click **Edit** to modify it.
- Step 3** Configure the optimization action list using the information in [Table 13-1](#).

**Table 13-1 Optimization Action List Configuration Options**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action List Name | Enter a unique name for the action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Enable Delta     | Delta optimization dynamically updates client browser caches directly with content differences, or deltas, resulting in faster page downloads.<br><br>Check this check box to enable delta optimization for the specified URLs.<br>Clear this check box to disable delta optimization for the specified URLs.<br><br><b>Note</b> The ACE restricts you from enabling delta optimization if you have previously specified either Cache Dynamic or Dynamic Entity Tag.                                                                                                                                                                                                                                                                                                        |
| Enable AppScope  | AppScope runs on the Management Console of the optional Cisco AVS 3180A Management Station and measures end-to-end application performance.<br><br>Check this check box to enable AppScope performance monitoring for use with the ACE appliance.<br>Clear this check box to disable AppScope performance monitoring for use with the ACE appliance.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Flash Forward    | The FlashForward feature reduces bandwidth usage and accelerates embedded object downloading by combining local object storage with dynamic renaming of embedded objects, thereby enforcing object freshness within the parent HTML page.<br><br>Specify how the ACE appliance is to implement FlashForward: <ul style="list-style-type: none"> <li>• N/A—Indicates that this feature is not enabled.</li> <li>• Flash Forward—Indicates that FlashForward is to be enabled for the specified URLs and that embedded objects are to be transformed.</li> <li>• Flash Forward Object—Indicates that FlashForward static caching is to be enabled for the objects that the corresponding URLs refer to, such as Cascading Style Sheets (CSS), JPEG, and GIF files.</li> </ul> |
| Cache Dynamic    | Check this check box to enable Adaptive Dynamic Caching for the specified URLs even if the expiration settings in the response indicate that the content is dynamic. The expiration of cache objects is controlled by the cache expiration settings based on time or server load.<br><br>Clear this check box to disable this feature.<br><br><b>Note</b> The ACE restricts you from enabling Cache Dynamic if you have previously specified either Enable Delta or Dynamic Entity Tag.                                                                                                                                                                                                                                                                                     |

**Table 13-1 Optimization Action List Configuration Options**

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cache Forward      | <p>Check this check box to enable the cache forward feature for the corresponding URLs. Cache forward allows the ACE to serve the object from its cache (static or dynamic) even when the object has expired if the maximum cache TTL time period has not yet expired (set by specifying the Cache Time-to-Live Duration (%): field in an Optimization parameter map). At the same time, the ACE sends an asynchronous request to the origin server to refresh its cache of the object.</p> <p>Clear this check box to disable this feature.</p>                                                        |
| Dynamic Entity Tag | <p>This feature enables the acceleration of noncacheable embedded objects, which results in improved application response time. When enabled, this feature eliminates the need for users to download noncacheable objects on each request.</p> <p>Check this check box to indicate that the ACE appliance is to implement just-in-time object acceleration for noncacheable embedded objects.</p> <p>Clear this check box to disable this feature.</p> <p><b>Note</b> The ACE restricts you from enabling Dynamic Entity Tag if you have previously specified either Enable Delta or Cache Dynamic.</p> |

**Step 4** Do the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to save your entries.

**Related Topics**

- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)
- [Configuring Optimization Parameter Maps, page 13-6](#)
- [Configuring Traffic Policies for HTTP Optimization, page 13-6](#)
- [Configuring Global Application Acceleration and Optimization, page 13-9](#)
- [Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 12-86](#)

# Configuring Optimization Parameter Maps

Use this procedure to configure an Optimization parameter map for use with a Layer 3/Layer 4 policy map.



## Tip

You can also configure optimization parameter maps when configuring a virtual server. For more information, see [Configuring Application Acceleration and Optimization, page 5-57](#).

## Procedure

- Step 1** Select **Config > Virtual Contexts > context > Load Balancing > Parameter Maps > Optimization Parameter Maps**. The Parameter Maps table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, and then click **Edit** to modify it. The Optimization Parameter Map configuration screen appears.
- Step 3** In the Parameter Name field, enter a unique name for this parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 32 alphanumeric characters.
- Step 4** Click **Optimization**. Optimization attributes appear.
- Step 5** Configure optimization using the information in [Table 8-5](#).
- Step 6** Do the following:
  - Click **Deploy Now** to save your entries. The ACE appliance validates the parameter map configuration and deploys it.
  - Click **Cancel** to exit this procedure without saving your entries and to return to the Parameter Map table.
  - Click **Next** to accept your entries and to add another parameter map.

## Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)
- [Configuring an HTTP Optimization Action List, page 13-3](#)
- [Configuring Traffic Policies for HTTP Optimization, page 13-6](#)
- [Configuring Global Application Acceleration and Optimization, page 13-9](#)

# Configuring Traffic Policies for HTTP Optimization

[Table 13-2](#) provides a high-level overview of the steps required to configure HTTP optimization on an ACE appliance.



## Note

[Table 13-2](#) includes only the significant steps in each task. For detailed information on configuring these items, select the links provided, click **Help** in the ACE Appliance Device Manager GUI, or refer to [Configuring Traffic Policies, page 12-1](#).

**Assumption**

A virtual IP address has been configured for the context in which you configure HTTP optimization.

**Table 13-2** *Configuring Traffic Policies for HTTP Optimization*

| Step   | Task                                                                                                                                                                                         | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Create a Layer 7 class map for server load balancing.                                                                                                                                        | <ol style="list-style-type: none"> <li>1. Select <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Class Maps</b>.</li> <li>2. Click <b>Add</b> to add a new class map.</li> <li>3. In the Class Map Type field, select <b>Layer 7 Server Load Balancing</b>.</li> <li>4. In the Match Type field, select the method the ACE appliance is to use to evaluate multiple match statements when multiple match conditions exist in the class map.</li> <li>5. Click <b>Deploy Now</b>.</li> <li>6. Configure match conditions for this class map.</li> </ol> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Virtual Context Class Maps, page 12-8</a></li> <li>• <a href="#">Setting Match Conditions for Layer 7 Server Load-Balancing Class Maps, page 12-16</a></li> </ul> |
| Step 2 | Create an HTTP optimization action list to specify the optimization actions that are to be performed.                                                                                        | <ol style="list-style-type: none"> <li>1. Select <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Action Lists</b>.</li> <li>2. Click <b>Add</b> to add a new action list.</li> <li>3. Configure the action list using the information in <a href="#">Table 13-1</a>.</li> <li>4. Click <b>Deploy Now</b>.</li> </ol> <p>For more information, see <a href="#">Configuring an HTTP Optimization Action List, page 13-3</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | Create a Layer 7 HTTP optimization policy map and associate it with the server load-balancing class map in <a href="#">Step 1</a> and the action list configured in <a href="#">Step 2</a> . | <ol style="list-style-type: none"> <li>1. Select <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Policy Maps</b>.</li> <li>2. Click <b>Add</b> to add a new policy map.</li> <li>3. In the Type field, select <b>Layer 7 HTTP Optimization</b>.</li> <li>4. Click <b>Deploy Now</b>.</li> <li>5. In the Rules table, add the server load-balancing class map created in <a href="#">Step 1</a>.</li> <li>6. In the Action table, add the action list created in <a href="#">Step 2</a>.</li> </ol> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Virtual Context Class Maps, page 12-8</a></li> <li>• <a href="#">Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 12-86</a></li> </ul>                                                        |

Table 13-2 Configuring Traffic Policies for HTTP Optimization (continued)

| Task                                                                                                                                                                                                                                                                                                                                                                                                           | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b><br>Create a Layer 3/Layer 4 class map for server load balancing.                                                                                                                                                                                                                                                                                                                                 | <ol style="list-style-type: none"> <li>1. Select <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Class Maps</b>.</li> <li>2. Click <b>Add</b> to add a new class map.</li> <li>3. In the Class Map Type field, select <b>Layer 3/4 Network Traffic</b>.</li> <li>4. In the Match Type field, select the method the ACE appliance is to use to evaluate multiple match statements when multiple match conditions exist in the class map.</li> <li>5. Click <b>Deploy Now</b>.</li> <li>6. Configure Virtual Address match conditions for this class map.</li> </ol> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Virtual Context Class Maps, page 12-8</a></li> <li>• <a href="#">Setting Match Conditions for Class Maps, page 12-10</a></li> </ul>                                                                                                                                                                  |
| <b>Step 5</b><br>Create a Layer 7 policy map for server load balancing and associate it with the Layer 7 server load-balancing class map from <a href="#">Step 1</a> .                                                                                                                                                                                                                                         | <ol style="list-style-type: none"> <li>1. Select <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Policy Maps</b>.</li> <li>2. Click <b>Add</b> to add a new policy map.</li> <li>3. In the Type field, select <b>Layer 7 Server Load Balancing</b>.</li> <li>4. Click <b>Deploy Now</b>.</li> <li>5. Associate the Layer 7 server load-balancing class map configured in <a href="#">Step 1</a> with this policy map by adding it to the Rule table.</li> </ol> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Virtual Context Policy Maps, page 12-34</a></li> <li>• <a href="#">Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 12-46</a></li> </ul>                                                                                                                                                                                                                            |
| <b>Step 6</b><br>Create a Layer 3/Layer 4 network traffic policy map and associate it with the: <ul style="list-style-type: none"> <li>• Layer 3/Layer 4 server load-balancing class map configured in <a href="#">Step 4</a></li> <li>• Layer 7 server load-balancing policy map configured in <a href="#">Step 5</a></li> <li>• HTTP optimization policy map configured in <a href="#">Step 3</a></li> </ul> | <ol style="list-style-type: none"> <li>1. Select <b>Config &gt; Virtual Contexts &gt; context &gt; Expert &gt; Policy Maps</b>.</li> <li>2. Click <b>Add</b> to add a new policy map.</li> <li>3. In the Type field, select <b>Layer 3/4 Network Traffic</b>.</li> <li>4. Click <b>Deploy Now</b>.</li> <li>5. In the Rule table, add the Layer 3/Layer 4 server load-balancing class map configured in <a href="#">Step 4</a>.</li> <li>6. In the Action table, add the:               <ul style="list-style-type: none"> <li>– Layer 7 server load-balancing policy map created in <a href="#">Step 5</a></li> <li>– HTTP optimization policy map created in <a href="#">Step 3</a></li> </ul> </li> </ol> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Virtual Context Policy Maps, page 12-34</a></li> <li>• <a href="#">Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 12-14</a></li> </ul> |



**Related Topics**

- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)
- [Configuring an HTTP Optimization Action List, page 13-3](#)
- [Optimization Overview, page 13-2](#)

## Enabling HTTP Optimization Using Virtual Servers

Use this procedure to configure HTTP optimization using virtual servers.

**Procedure**

- 
- |               |                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Create a virtual server by following the instructions in <a href="#">Configuring Virtual Contexts, page 4-1</a> .                               |
| <b>Step 2</b> | Configure HTTP optimization by following the instructions in <a href="#">Configuring Application Acceleration and Optimization, page 5-57</a> . |
- 

**Related Topics**

- [Configuring Traffic Policies for HTTP Optimization, page 13-6](#)
- [Configuring Optimization Parameter Maps, page 13-6](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)

## Configuring Global Application Acceleration and Optimization

**Note**

This functionality is available for only Admin contexts.

ACE Appliance Device Manager allows you to configure global application acceleration and optimization options for logging and debugging as performed by the ACE appliance.

**Procedure**

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select <b>Config &gt; Virtual Contexts &gt; <i>admin_context</i> &gt; System &gt; Application Acceleration And Optimization</b> . The Application Acceleration And Optimization configuration screen appears.                                                                                                                                                                          |
| <b>Step 2</b> | In the Debug Level field, enter the maximum level of system log messages to be sent to the syslog server, using the values in <a href="#">Table 4-4</a> . The severity level that you specify indicates that you want syslog messages at that level and the more severe levels. For example, if you enter 3 for Error, syslog displays Error, Critical, Alert, and Emergency messages. |
| <b>Step 3</b> | Check the Appscope Log check box to indicate that the ACE appliance is to upload optimization statistical log information to the optional AVS 3180A Management station. Clear the check box to indicate that the ACE appliance is not to upload this information.                                                                                                                      |

**Step 4** Click **Deploy Now** to deploy this configuration on the ACE appliance.

---

**Related Topics**

- [Optimization Overview, page 13-2](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 13-2](#)



# CHAPTER 14

## Monitoring Your Network

---

The ACE Appliance Device Manager Monitor function allows you to monitor key areas of system usage. The following functionality is provided under the Monitor tab:

- [Using Dashboards to Monitor the ACE System and Virtual Contexts, page 14-2](#)
- [Error Monitoring, page 14-15](#)
- [Monitoring Resource Usage, page 14-17](#)
- [Monitoring Traffic, page 14-21](#)
- [Monitoring Load Balancing, page 14-23](#)
- [Monitoring Application Acceleration, page 14-29](#)
- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts, page 14-31](#)
- [Setting Up Virtual Contexts Statistics Collection, page 14-33](#)
- [Displaying Network Topology Maps, page 14-34](#)
- [Testing Ping, page 14-36](#)



### Note

To troubleshoot problems related to the ACE appliance, use the **debug** and **show** commands supported in the command line interface (CLI). For a list of the ACE appliance **show** commands, see the *Command Reference, Cisco ACE Application Control Engine*. For more detailed descriptions of hardware and software show commands, see the *Administration Guide, Cisco ACE Application Control Engine*.



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

### Prerequisite

Before using the Monitoring functions, you must:

- Enable monitoring on the virtual contexts or servers (see [Setting Up Virtual Contexts Statistics Collection, page 14-33](#) and [Monitoring Load Balancing on Probes, page 14-27](#) or the *Administration Guide, Cisco ACE Application Control Engine*).

- Ensure that you allow the SNMP protocol and enter the v2c community string in the **Config > System > Primary Attributes** page.
- Select the virtual context you want to monitor. This step is reflected in the monitoring procedures as part of selecting your task; such as **Monitor > Virtual Contexts > context > Load Balancing**.

## Using Dashboards to Monitor the ACE System and Virtual Contexts

DM dashboards allow for faster and more accurate assessment and analysis of the ACE system and virtual context health and usage, as well as performance. Corresponding monitoring views allow for quick access to details for further investigation into potential problems highlighted in the dashboards. Graphs, as well as monitoring screens, allow you to view historical data and compare the performance with the peer objects.



### Note

All client browsers require that you enable Adobe Flash Player 9 to properly display the monitoring graphs provided in DM.

Dashboards in DM provide:

- A central location for you to view monitoring highlights.
- Emphasis on potential issues that require your attention.
- Quick access to relevant DM pages for more detailed monitoring data.

In each dashboard, there are a relevant set of dashboard panes. The dashboard panes are moveable element inside the dashboard that can be minimized/maximized, moved, and, if desired, removed from view. You can also display a larger (full) window view for a dashboard window.



### Note

Changes made to dashboard layout or pane selections are only applicable for the current session. Those changes are not maintained by DM the next time you access an DM dashboard.

The dashboard tables and graphs autorefresh at each sync. If desired, you can disable autofreshing by clicking the Pause Autofresh button in the upper-right corner of the dashboard.



### Note

All dashboard contents are under Role-Based Access Control (RBAC). Options will be grayed or not displayed if proper permission has not been granted to the logged in user by the administrator. See the [“Controlling Access to the Cisco ACE Appliance” section on page 15-3](#) for more information about RBAC in DM.

This section includes the following topics:

- [ACE System Dashboard, page 14-3](#)
- [ACE Virtual Context Dashboard, page 14-11](#)

## ACE System Dashboard

The ACE System Dashboard displays the information related to the ACE appliance. You access the ACE System Dashboard by selecting **Monitor > Virtual Contexts > Dashboard > System Dashboard**.

To enhance your viewing of the monitoring information in the ACE System Dashboard, you can perform the following actions:

- Click and drag an individual dashboard pane to move it to another location within the ACE System Dashboard.
- Use the Collapse/Expand buttons at the top right side of each dashboard pane to minimize/maximize a pane within the ACE System Dashboard.
- Click the **Remove** button to remove a dashboard pane from the ACE System Dashboard. Click the **Refresh Now** button at the top of the ACE System Dashboard to open the closed dashboard pane.



---

**Note**

When you close any of the panes in a dashboard by clicking the Remove button, all of the headers in the other dashboard panes turn black to indicate that a pane has been closed. To return the dashboard panes to normal, click the **Refresh Now** button to reload the removed dashboard pane.

---

- Click the **Screen View (Full)/Screen View (Normal)** buttons to display a larger (full) window view for the ACE Dashboard.

Changes made to dashboard layout or pane selections are only applicable for the current session. Those changes are not maintained by DM the next time you access the ACE System Dashboard.

The components of the individual ACE System Dashboard panes are described in the following sections.

- [Device Information Table, page 14-4](#)
- [License Status Table, page 14-4](#)
- [High Availability Table, page 14-5](#)
- [Device Configuration Summary Table, page 14-5](#)
- [Context With Denied Resource Usage Detected Table, page 14-7](#)
- [Device Resource Usage Graph, page 14-7](#)
- [Top 10 Current Resources Table, page 14-8](#)
- [Control Plane CPU/Memory Graphs, page 14-10](#)

## Device Information Table

The Device Information table lists the details that will identify the status of the selected ACE. It includes the following fields:

- Host Name—Host name of the ACE appliance.
- Device Status—Device reachability status through SNMP and XML connectivity (Up or Down).
- Device Type—ACE device specifics for the ACE appliance.
- Management IP—Management IP address of the admin virtual context.
- Number of Contexts—Number of configured contexts, including the Admin context and configured user contexts.
- Software Version—Release software version of the ACE appliance.
- Last Boot Reason—Reason for the last reboot of the ACE (if available).
- Uptime—Length of time that the ACE has been up and running.

The data shown in this table is collected during device discovery as well as during periodic monitor polling. The timestamp shown in the status bar is from the last polled time of the Admin virtual context.

## License Status Table

The License Status table lists the license status of the ACE appliance. DM uses the ACE **show license status** CLI command to obtain the license details. The timestamp shown in the status bar is from the last polled time of the Admin virtual context.

## High Availability Table

The HA Peer Information table lists the details of the HA peer, if configured in HA mode. It includes the following information:

- HA/FT Interface State—State of the local ACE. See the [“High Availability Polling” section on page 11-2](#).
- My IP Address—IP address of the local ACE.
- Peer IP Address—IP address of the peer ACE.
- Software Compatibility—Status of whether the software version of the local ACE and the software version of the peer ACE are compatible. Possible states are the INIT, COMPATIBLE, or INCOMPATIBLE state.
- License Compatibility—Status of whether the license of the local ACE and the license of the peer ACE are compatible. Possible states are the INIT, COMPATIBLE, or INCOMPATIBLE state.
- Number of FT Groups—Number of configured FT groups.
- Number of Heartbeats Transmitted—Total number of heartbeat packets transmitted.
- Number of Heartbeats Received—Total number of heartbeat packets received.

This data is collected during periodic monitoring polling. The timestamp shown in the status bar is from the last polled time of the Admin virtual context.

## Device Configuration Summary Table

The Device Configuration Summary table displays the following information:

- Virtual Servers—Total count of virtual servers configured in all contexts and the count of virtual servers that are in the In Service or Out of Service state. DM also identifies virtual servers that have a Status Not Available state (due to polled failing, polled disable, and so on) and have a Status Not Supported state (due to a lack of SNMP support on the ACE appliance). A hyperlink enables you to view load balancing virtual server monitoring information based on the identified state (see the [“Monitoring Load Balancing on Virtual Servers” section on page 14-23](#)). For example, if you click the In Service hyperlink, you will see only the virtual servers that are currently in service.
- Real Servers—Total count of real servers configured in all contexts and the count of real servers that are in In Service and Out of Service. A hyperlink enables you to view load balancing real server monitoring information based on the identified state (see the [“Monitoring Load Balancing on Real Servers” section on page 14-25](#)). For example, if you click the In Service hyperlink, you will see only the real servers that are currently in service.
- Probes—Total count of probes configured in all contexts and the count of probes that are in the In Service and Out of Service state. A hyperlink enables you to view load balancing probe monitoring information based on the identified state (see the [“Monitoring Load Balancing on Probes” section on page 14-27](#)). For example, if you click the In Service hyperlink, you will see only the probes that are currently in service.
- Gigabit Ethernet—Total count of Gigabit Ethernet physical interfaces configured on the ACE appliance based on their operational status of Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the Gigabit Ethernet physical interfaces that currently have an operational status of Up.

- **VLANs**—Total count of VLANs configured and the count of VLANs based on operational status - Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the VLAN interfaces that currently have an operational status of Up.
- **Port Channels**—Total count of port channels configured on the ACE appliance based on their operational status of Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the port channels that currently have an operational status of Up.
- **BVIs**—Total count of BVI interfaces and the count of BVI interfaces based on their operational status of Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the BVI interfaces that currently have an operational status of Up.
- **Certificates**—Total count of SSL certificates and the count of SSL certificates that are expiring beyond 30 days, expired, or that are expiring within 30 days. A hyperlink accesses a popup window for you to view the SSL certificates list based on the selection, displaying the certificate name, device name, days to expire, expiration date, and the date it was evaluated for you to determine the days to expire. Certificates are considered expired if their expiration date is within the next day (rounded down the next day). A hyperlink in the device name allows you to navigate to the context-based SSL Certificate configuration page (see the [“Using SSL Certificates” section on page 9-6](#)).

**Note**

The Certificates information does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version” section on page 1-2](#)).

This data is collected during discovery as well as during periodic monitoring polling. The timestamp shown in the status bar indicates a varying poll time; that is, different virtual contexts were polled and those context had different time stamps. The earliest time stamp of the polled virtual contexts is displayed in the status bar.

All counts shown in the Device Configuration Summary table are based on the operational status of the monitored objects listed above.

- **Out Of Service**—Indicates any status other than In Service (for example, Out Of Service, Failed, or Disabled).
- **Status not available**—Indicates that DM was unable to poll the operational status of this object. The display of this operational status could be due to polling errors or the device was unreachable. Also, if a poll was recently initiated, this operational status could indicate that DM is in the process of collecting data.
- **Status not supported**—Indicates that the device does not have the capability to provide an operational status of this object. The display of this operational status could be due to missing SNMP instrumentation on the ACE appliance.



## Context With Denied Resource Usage Detected Table

The Context With Denied Resource Usage Detected table lists all contexts for which the resource request is denied after reaching the maximum limit. An increase in the deny count (that is, the deny rate) results in the relevant context resource type appearing in this table. DM obtains the count information by using the ACE **show resource usage** CLI command, which collects the information from the following MIBs: `crlResourceLimitReqsDeniedCount` and `crlRateLimitResourceReqsDeniedCount`.

This table includes the following information:

- Context—Name of the configured context that contains a denied resource.
- Resource Type—Type of system resource in the context.
- Denies/Second—Number of denied resources (per second) as a result of oversubscription or resource depletion.
- Total Deny Count—Number of denied uses of the resource since the resource statistics were last cleared.
- Last Polled Count—Date and time of the last time that DM polled the device to display the current values.

**Note**

The Context With Denied Resource Usage Detected table does not display the sticky denied resource count because this count does not increment when the ACE sticky resources are exhausted. The ACE sticky table can hold a maximum of four million entries (four million simultaneous users). When the table reaches the maximum number of entries, additional sticky connections cause the table to wrap and the first users become unstuck from their respective servers.

A hyperlink allows you to access the Resource Usage monitoring page to view a detailed list of resources used and denied counts (see the [“Monitoring Resource Usage” section on page 14-17](#)).

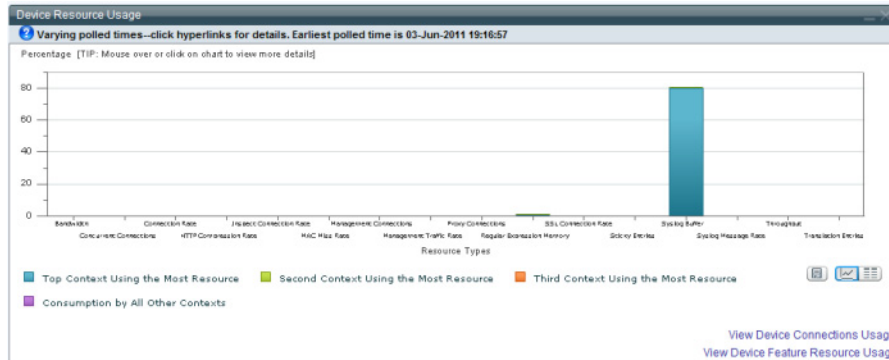
## Device Resource Usage Graph

For each resource type, the ACE System Dashboard displays the Top 3 virtual contexts that consume the resources in the Device Resource Usage graph ([Figure 14-1](#)). A tooltip is added to display the Top 3 context names and their consumption, consumption of the resource by rest of the contexts and the total consumption by all contexts. This data is collected by DM by using the ACE **show resource usage** CLI command.

**Note**

The SSL Connection Rate graph entry does not apply to the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version” section on page 1-2](#)).

The timestamp shown in the status bar indicates a varying poll time; that is, different virtual contexts were polled and those context had different time stamps. The earliest time stamp of the polled virtual contexts is displayed in the status bar.

**Figure 14-1** Device Resource Usage Graph

To toggle the display of the Device Resource Usage graph in the monitoring window:

- Click **View As Chart** to display the object data as a graph.
- Click **View As Grid** to display the object data as a numerical line grid.

**Note**

If you want to save the graph as a JPEG file for archive or other purposes, click the **Show As Image** button. When you mouse over the graph, the Image Toolbar appears. From the Image Toolbar, you can save the graph as a JPEG or send it in an email. You can also print the graph if desired.

If you want to export object data to Microsoft Excel for archive or other purposes, click the **Export to Excel** link in the View As Grid object display.

Hyperlinks allow you to access the individual resource usage page for more details (see the “[Monitoring Resource Usage](#)” section on page 14-17).

**Note**

ACL Memory and Application Acceleration for the ACE appliance do not appear in the Device Resource Usage graph. To view the detailed counters, click the hyperlink to access individual resource usage page.

## Top 10 Current Resources Table

The Top 10 Resource Usage table ([Figure 14-2](#)) displays the Top 10 resource types that have been evaluated for high resource utilization. The resource with highest utilization appears at the top. This data is collected by DM by using the ACE **show resource usage** CLI command.

**Figure 14-2** Top 10 Current Resources Table—ACE Dashboard

| Top 10 Current Resources |                                          |             |                           |         |         |                      |
|--------------------------|------------------------------------------|-------------|---------------------------|---------|---------|----------------------|
| Last Hour                | Resource Name                            | Used By     | Current Usage             | Avg.    | Max.    | Last Polled Time     |
|                          | Syslog Buffer Size (Bytes)               | Global Pool | 80.664% (845824/1048576)  | 77.486% | 80.664% | 03-Jun-2011 19:16:57 |
|                          | ACL Memory (Bytes)                       | Global Pool | 2.448% (1195264/48824320) | 2.448%  | 2.448%  | 03-Jun-2011 19:16:57 |
|                          | Regular Expression Memory (Bytes)        | Global Pool | 1.150% (12061/1048576)    | 1.150%  | 1.150%  | 03-Jun-2011 19:16:57 |
|                          | Management Connection Rate (Connections) | Admin       | 0.550% (28/5095)          | 0.546%  | 0.707%  | 03-Jun-2011 19:16:57 |
|                          | Syslog Message Rate (Messages/Sec)       | Global Pool | 0.004% (4/100000)         | 0.002%  | 0.004%  | 03-Jun-2011 19:16:57 |
|                          | Concurrent Connections (Connections)     | Admin       | 0.002% (2/100095)         | 0.002%  | 0.002%  | 03-Jun-2011 19:16:57 |
|                          | Application Acceleration (Connections)   | Global Pool | 0.000% (0/105)            | 0.000%  | 0.000%  | 03-Jun-2011 19:16:57 |
|                          | Bandwidth (Bytes/Sec)                    | Global Pool | 0.000% (0/244342000)      | 0.000%  | 0.000%  | 03-Jun-2011 19:16:57 |
|                          | Concurrent Connections (Connections)     | Global Pool | 0.000% (0/1899905)        | 0.000%  | 0.000%  | 03-Jun-2011 19:16:57 |
|                          | Connection Rate (Connections/Sec)        | Global Pool | 0.000% (0/119900)         | 0.000%  | 0.000%  | 03-Jun-2011 19:16:57 |

This table includes the following information:

- Last Hour—Plot of high resource utilization during the past hour.
- Resource Name—Type of system resource in the context.
- Used By—Name of the virtual context that is placing the high demands on the resource. The Global Pool usage is critical in the setup where one or more contexts are configured to make use of the global pool once their reserved resource are depleted and resource is free in the global pool. In this situation, if the global pool is depleted, multiple contexts may be starved for resource.




---

**Note** Contexts configured to make use of the global pool will not be evaluated for the Top 10 Resource Usage table.

---

- Current Usage—Active concurrent instances or the current rate of the resource.
- Average—Average value of resource usage (based on the last hour).
- Max.—Highest value of resource usage (based on the last hour).
- Last Polled—Date and time of the last time that DM polled the device to display the current values.

Hyperlinks allow you to access the individual resource usage page for more details (see the [“Monitoring Resource Usage”](#) section on page 14-17).

## Control Plane CPU/Memory Graphs

The Control Plane CPU/Memory graphs (Figure 14-3) show the utilization of the ACE CPU. This data consists of two graphs:

- The Control Plane CPU Usage graph shows the utilization of the ACE CPU as a percentage.
- The Control Plane Memory graph displays the consumed memory on Kbytes. A tooltip is added to display the Cache Memory, Total Memory, Shared Memory, Buffer Memory, and Free Memory usage as a percentage.

To toggle the display of the Control Plane CPU/Memory graph in the monitoring window:

- Click **View As Chart** to display the object data as a graph.
- Click **View As Grid** to display the object data as a numerical line grid.

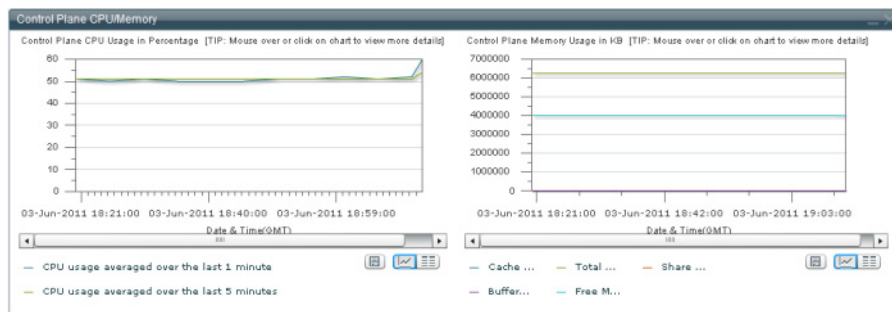


### Note

If you want to save the graph as a JPEG file for archive or other purposes, click the **Show As Image** button. When you mouse over the graph, the Image Toolbar appears. From the Image Toolbar, you can save the graph as a JPEG or send it in an email. You can also print the graph if desired.

If you want to export object data to Microsoft Excel for archive or other purposes, click the **Export to Excel** link in the View As Grid object display.

**Figure 14-3** Control Plane CPU/Memory Graphs



## ACE Virtual Context Dashboard

The ACE Virtual Context Dashboard displays monitoring information for an ACE virtual context selected from the device tree. You access the ACE Virtual Context Dashboard by selecting **Monitor > Virtual Contexts > Context Dashboard**.

To enhance your viewing of the monitoring information in the ACE Virtual Context Dashboard, you can perform the following actions:

- Click and drag an individual dashboard pane to move it to another location within the ACE Virtual Context Dashboard.
- Use the Collapse/Expand buttons at the top right side of each dashboard pane to minimize/maximize a pane within the ACE Virtual Context Dashboard.
- Click the **Remove** button to remove a dashboard pane from the ACE Virtual Context Dashboard. Click the **Refresh Now** button at the top of the ACE Virtual Context Dashboard to open the closed dashboard pane.

**Note**

When you close any of the panes in a dashboard by clicking the Remove button, all of the headers in the other dashboard panes turn black to indicate that a pane has been closed. To return the dashboard panes to normal, click the **Refresh Now** button to reload the removed dashboard pane.

- Click the **Screen View (Full)/Screen View (Normal)** buttons to display a larger (full) window view for the ACE Dashboard.

Changes made to dashboard layout or pane selections are only applicable for the current session. Those changes are not maintained by DM the next time you access the ACE Virtual Context Dashboard.

The components of the individual ACE Virtual Context Dashboard panes are described in the following sections.

- [Device Configuration Summary Table, page 14-12](#)
- [Context With Denied Resource Usage Detected Table, page 14-13](#)
- [Context Resource Usage Graph, page 14-14](#)
- [Load Balancing Servers Performance Graphs, page 14-14](#)

## Device Configuration Summary Table

The Device Configuration Summary table displays the following information:

- **Virtual Servers**—Total count of virtual servers configured in all contexts and the count of virtual servers that are in the In Service and Out of Service state. DM also identifies virtual servers that have a Status Not Available state (due to polled failing, polled disable, and so on) and have a Status Not Supported state (due to a lack of ACE SNMP support). A hyperlink enables you to view load balancing virtual server monitoring information based on the identified state (see the [“Monitoring Load Balancing on Virtual Servers” section on page 14-23](#)). For example, if you click the In Service hyperlink, you will see only the virtual servers that are currently in service.
- **Real Servers**—Total count of real servers configured in all contexts and the count of real servers that are in In Service and Out of Service. A hyperlink enables you to view load balancing real server monitoring information based on the identified state (see the [“Monitoring Load Balancing on Real Servers” section on page 14-25](#)). For example, if you click the In Service hyperlink, you will see only the real servers that are currently in service.
- **Probes**—Total count of probes configured in all contexts and the count of probes that are in the In Service and Out of Service state. A hyperlink enables you to view load balancing probe monitoring information based on the identified state (see the [“Monitoring Load Balancing on Probes” section on page 14-27](#)). For example, if you click the In Service hyperlink, you will see only the probes that are currently in service.
- **Gigabit Ethernet**s—Total count of Gigabit Ethernet physical interfaces configured on the ACE appliance based on their operational status of Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the Gigabit Ethernet physical interfaces that currently have an operational status of Up.
- **VLAN**s—Total count of VLANs configured and the count of VLANs based on operational status - Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the VLAN interfaces that currently have an operational status of Up.
- **Port Channels**—Total count of port channels configured on the ACE appliance based on their operational status of Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the port channels that currently have an operational status of Up.
- **BVI**s—Total count of BVI interfaces and the count of BVI interfaces based on their operational status of Up and Down. A hyperlink enables you to view traffic summary information based on the identified state (see the [“Monitoring Traffic” section on page 14-21](#)). For example, if you click the Up hyperlink, you will see only the BVI interfaces that currently have an operational status of Up.

- **Certificates**—Total count of SSL certificates and the count of SSL certificates that are expiring beyond 30 days, expired, or that are expiring within 30 days. A hyperlink accesses a popup window for you to view the SSL certificates list based on the selection, displaying the certificate name, device name, days to expire, expiration date, and the date it was evaluated for you to determine the days to expire. Certificates are considered expired if their expiration date is within the next day (rounded down the next day). A hyperlink in the device name allows you to navigate to the context-based SSL Certificate configuration page (see the [“Using SSL Certificates” section on page 9-6](#)).

Counts are based on the selected ACE virtual context and not for all ACE virtual contexts.

This data is collected during discovery as well as during periodic monitoring polling. The timestamp shown in the status bar indicates a varying poll time; that is, different virtual contexts were polled and the contexts had different time stamps. The earliest time stamp of the polled virtual contexts is displayed in the status bar.

All counts shown in the Device Configuration Summary table are based on the operational status of the monitored objects listed above.

- **Out Of Service**—Indicates any status other than In Service (for example, Out Of Service, Failed, or Disabled).
- **Status not available**—Indicates that DM was unable to poll the operational status of this object. The display of this operational status could be due to polling errors or the device was unreachable. Also, if a poll was recently initiated, this operational status could indicate that DM is in the process of collecting data.
- **Status not supported**—Indicates that the device does not have the capability to provide an operational status of this object. The display of this operational status could be due to missing SNMP instrumentation on the ACE appliance.

## Context With Denied Resource Usage Detected Table

The Context With Denied Resource Usage Detected table lists all contexts for which the resource request is denied after reaching the maximum limit. An increase in the deny count (that is, the deny rate) will result in the relevant context resource type to appear in this table. This data is collected by DM by using the ACE **show resource usage** CLI command.

This table includes the following information:

- **Context**—Name of the configured context that contains a denied resource.
- **Resource Type**—Type of system resource in the context.
- **Denies/Second**—Number of denied resources (per second) as a result of oversubscription or resource depletion.
- **Total Deny Count**—Number of denied uses of the resource since the resource statistics were last cleared.
- **Last Polled**—Date and time of the last time that DM polled the device to display the current values.



**Note**

This information is collected from the following MIBs: `crlResourceLimitReqsDeniedCount` and `crlRateLimitResourceReqsDeniedCount`.

A hyperlink allows you to access the Resource Usage monitoring page to view a detailed list of resources used and denied counts (see the [“Monitoring Resource Usage” section on page 14-17](#)).

## Context Resource Usage Graph

The Context Resource Usage graph displays the details of each resource type utilized by the selected contexts. For each resource type, the graph includes the following monitoring statistics: Used, Global Available, and Guaranteed. This data is collected by DM by using the ACE **show resource usage** CLI command.

To toggle the display of the Context Resource Usage graph in the monitoring window:

- Click **View As Chart** to display the object data as a graph.
- Click **View As Grid** to display the object data as a numerical line grid.

**Note**

If you want to save the graph as a JPEG file for archive or other purposes, click the **Show As Image** button. When you mouse over the graph, the Image Toolbar appears. From the Image Toolbar, you can save the graph as a JPEG or send it in an email. You can also print the graph if desired.

If you want to export object data to Microsoft Excel for archive or other purposes, click the **Export to Excel** link in the View As Grid object display.

Hyperlinks allow you to access the individual resource usage page for more details (see the [“Monitoring Resource Usage” section on page 14-17](#)).

**Note**

ACL Memory and Application Acceleration for the ACE appliance do not appear in the Device Resource Usage graph. To view the detailed counters, click the hyperlink to access individual resource usage page.

## Load Balancing Servers Performance Graphs

The Load Balancing Servers Performance graphs ([Figure 14-4](#)) include:

- **Top 5 Virtual Servers**—Displays the top five virtual servers in the selected virtual context. You can select from server statistics (such as High Connection Rate, Dropped Connection Rate, and so on) that are collected by DM polling for top performance evaluation.
- **Top 5 Real Servers**—Displays the top five real servers in the selected virtual context. You can select from server statistics (such as High Connection Rate, Dropped Connection Rate, and so on) that are collected by DM polling for top performance evaluation.

You select the statistic from the Select Statistics drop-down list.

To toggle the display of a Load Balancing Servers Performance graph in the monitoring window:

- Click **View As Chart** to display the object data as a graph.
- Click **View As Grid** to display the object data as a numerical line grid.

**Note**

If you want to save the graph as a JPEG file for archive or other purposes, click the **Show As Image** button. When you mouse over the graph, the Image Toolbar appears. From the Image Toolbar, you can save the graph as a JPEG or send it in an email. You can also print the graph if desired.

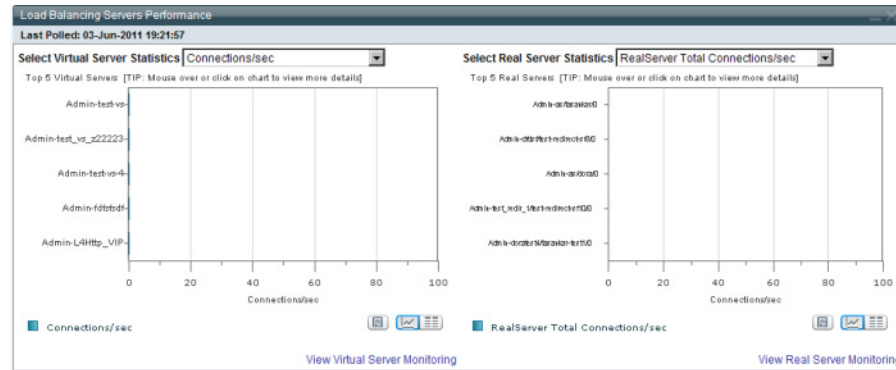
If you want to export object data to Microsoft Excel for archive or other purposes, click the **Export to Excel** link in the View As Grid object display.



Hyperlinks allow you to access the corresponding monitoring screens for more details:

- [Monitoring Load Balancing on Virtual Servers, page 14-23](#)
- [Monitoring Load Balancing on Real Servers, page 14-25](#)

**Figure 14-4** Load Balancing Servers Performance Graphs



## Error Monitoring

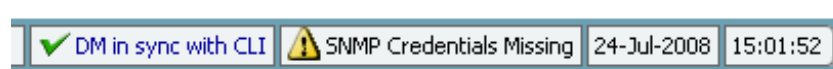
Error monitoring displays virtual context-specific runtime polling state error messages in the bottom right status bar of the DM GUI (see [Figure 14-5](#)). [Table 14-1](#) lists the polling states and actions required to resolve them. Device Manager and CLI synchronization status messages also display in this same location for the active context.



### Note

Time values are displayed using a fixed time zone (GMT). The Device Manager automatically converts the timezone setting of the ACE appliance to GMT and displays the GMT string adjacent to the current time.

**Figure 14-5** Polling State Message Location



**Table 14-1** Polling Error States

| Polling States           | Action Required                                                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polling Started          | No action required. Everything is working properly. Polling states will display activity. This state is not displayed in the interface.                |
| SNMP Credentials Missing | SNMP credentials are not configured for this virtual context; therefore, statistics are not collected. Add the SNMP v2c credentials to fix this error. |

**Table 14-1**      *Polling Error States*

| Polling States    | Action Required                                                                                                                                                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polling Timed Out | SNMP polling has timed out. This may occur if the wrong credentials were configured or may be caused by an internal error (such as SNMP protocol configured incorrectly or destination is not reachable). Verify that SNMP credentials are correct. If the problem persists, enable the SNMP collection again. |
| Polling Failed    | SNMP polling failed due to some internal error. Try enabling the SNMP collection again.                                                                                                                                                                                                                        |
| Not Polled        | SNMP polling has not started. This happens when the virtual context is first created from ACE Appliance Device Manager and the SNMP credentials are not configured. Add the SNMP v2c credentials to fix this error.                                                                                            |
| Unknown           | SNMP polling is not working due to one of the above-mentioned conditions. Check the SNMP v2c credential configuration.                                                                                                                                                                                         |

These states are only applicable for the SNMP polling done per virtual context. Statistics collected for the ACE Appliance Device Manager processes (shown under Admin > Device Management) are not collected via SNMP.

#### Related Topics

- [Monitoring Your Network, page 14-1](#)
- [Viewing Virtual Context Synchronization Status, page 4-80](#)
- [Monitoring ACE Appliance Statistics, page 15-35](#)

# Monitoring Resource Usage

DM provides resource usage so that you can easily determine if you need to reallocate resources to a particular virtual context, view traffic usage in your contexts, or determine available usage for your contexts. There are three modes in which DM provides resource usage for ACEs:

- Virtual-context based resource usage—You must choose **Monitor > Virtual Contexts > Resource Usage > Resource Usage** and select a virtual context from the top-right drop-down menu to view resource usage specific to the context (see the “[Monitoring Virtual Context Resource Usage](#)” section on page 14-17).
- System-wide resource usage—You must choose **Monitor > Virtual Contexts > Resource Usage** to view system-wide information and to display the following options:
  - Connections—Displays traffic resource usage information. See the “[Monitoring System Traffic Resource Usage](#)” section on page 14-19.
  - Features—Displays non-connection based resource usage information. See the “[Monitoring System Non-Connection Based Resource Usage](#)” section on page 14-20.
- Dashboard usage—You can choose either **Monitor > Virtual Contexts > Context Dashboard** or **Monitor > Virtual Contexts > System Dashboard**. See the “[Using Dashboards to Monitor the ACE System and Virtual Contexts](#)” section on page 14-2.

See the “Configuring Virtualization” chapter of the *Virtualization Guide, Cisco ACE Application Control Engine* for the maximum resource usage value for each attribute.

## Monitoring Virtual Context Resource Usage

DM displays resource usage for virtual contexts as explained in the following steps.

See the “Configuring Virtualization” chapter in the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide* for the maximum resource usage value for each attribute.

### Procedure

---

**Step 1** Choose **Monitor > Virtual Contexts > Resource Usage > Resource Usage**.

**Step 2** Use the object selector to view resource usage specific to the context.

The information in [Table 14-2](#) is displayed.




---

**Note** There might be a slight delay because the resource usage information is gathered real-time from the ACE appliance.

---

Table 14-2 Context Resource Usage Fields


| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource             | <p>List of resources which can be:</p> <ul style="list-style-type: none"> <li>• <b>acc-connections</b>—Number of acceleration connections</li> <li>• <b>acl-memory</b>—Memory space allocated for ACLs</li> <li>• <b>bandwidth</b>—Context throughput in bytes per second. The total bandwidth rate of a context consists of the following two resource usage fields: <ul style="list-style-type: none"> <li>– <b>throughput</b>—Displays through-the-ACE traffic. This is a derived value (you cannot configure it directly) and it is equal to the bandwidth rate minus the mgmt-traffic rate for the 1-Gbps and 2-Gbps licenses.</li> <li>– <b>mgmt-traffic</b>—Displays management (to-the-ACE) traffic in bytes per second. To guarantee a minimum amount of management traffic bandwidth, you must explicitly allocate a minimum percentage to management traffic using the rate mgmt-traffic parameter. When you allocate a minimum percentage of bandwidth to management traffic, the ACE subtracts that value from the maximum available management traffic bandwidth for all contexts in the ACE.</li> </ul> </li> <li>• <b>conc-connections</b>—Number of simultaneous connections</li> <li>• <b>connection rate</b>—Number of connections of any kind per second</li> <li>• <b>http-comp rate</b>—Compression rate for HTTP-based traffic in connections per second</li> <li>• <b>inspect-conn rate</b>—Number of application protocol inspection connections per second for FTP and RTSP only</li> <li>• <b>mac-miss rate</b>—To-the-ACE traffic sent to the control plane when the encapsulation is not correct in bytes per second</li> <li>• <b>mgmt-connections</b>—Number of management (to-the-ACE) connections</li> <li>• <b>mgmt-traffic rate</b>—Management to-the-ACE traffic in bytes per second</li> <li>• <b>proxy-connections</b>—Number of proxy connections</li> <li>• <b>regex</b>—Amount of regular expression memory</li> <li>• <b>ssl-connections rate</b>—Number of SSL connections per second</li> </ul> <p> <b>Note</b> The ssl-connections rate resource does not display with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> <ul style="list-style-type: none"> <li>• <b>sticky</b>—Displays the resource usage for the sticky entries.</li> </ul> <p><b>Note</b> If a context has fewer sticky resources than the configured Allocation Minimum, the ACE displays the Actual Minimum value that you can assign to the context.</p> <ul style="list-style-type: none"> <li>• <b>syslog buffer</b>—Number of syslog buffers</li> <li>• <b>syslog rate</b>—Number of syslog messages per second</li> <li>• <b>xlates</b>—Number of network and port address translations entries</li> </ul> |
| Current              | Displays the current resource usage.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Guaranteed Available | Indicates resource units that are guaranteed to be available to each context.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 14-2 Context Resource Usage Fields (continued)

| Field            | Description                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Shared Available | Indicates number of resource units that might be available to each context and are shared among all contexts from the oversubscription pool. |
| Denied           | Number of denied resources because of oversubscription or resource depletion.                                                                |

**Step 3** Click **Poll Now** to instruct DM to poll the devices and display the current values, and click **OK** when prompted if you want to poll the devices for data now.

**Step 4** Click **Graph** to display a historical trend graph of resource data for the virtual context (see the “Configuring Historical Trend and Real Time Graphs for Virtual Contexts” section on page 14-31 for details).

#### Related Topics

- [Monitoring System Traffic Resource Usage, page 14-19](#)
- [Monitoring System Non-Connection Based Resource Usage, page 14-20](#)
- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts, page 14-31](#)

## Monitoring System Traffic Resource Usage

DM displays system-wide traffic resource usage as explained in the following steps. See the “Configuring Virtualization” chapter in the *Virtualization Guide, Cisco ACE Application Control Engine* for the maximum resource usage value for each attribute.

#### Procedure

**Step 1** Choose **Monitor > Virtual Contexts > Resource Usage > Connections**.

The current resource usage information appears as shown in [Table 14-3](#).




**Note** There might be a slight delay because the resource usage information is gathered in real-time.

Table 14-3 System Resource Usage Connections Field Descriptions

| Field                  | Description                        |
|------------------------|------------------------------------|
| Context                | Name of the virtual context        |
| Conc. Conn. %          | Number of simultaneous connections |
| Mgmt. Conn. %          | Number of management connections   |
| Proxy Conn. %          | Proxy connections                  |
| Bandwidth (Bytes/S) %  | Bandwidth in bytes per second      |
| Throughput (Bytes/S)   | Throughput in bytes per second     |
| Conn. Rate (Conn./S) % | Connections per second             |

Table 14-3 System Resource Usage Connections Field Descriptions (continued)

| Field                          | Description                                                                                                                                                                                                                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSL Conn. Rate (Trans./S) %    | SSL (Secure Sockets Layer) connections per second                                                                                                                                                                                                                                           |
|                                |  <b>Note</b> The SSL Conn. Rate field does not display with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2). |
| Mgmt. Traffic Rate (Conn./S) % | Management traffic connections per second                                                                                                                                                                                                                                                   |
| MAC Miss Rate (Conn./S) %      | MAC miss traffic punted to CP packets per second                                                                                                                                                                                                                                            |
| Insp. Conn. Rate (Conn./S) %   | RTSP/FTP inspection connections per second                                                                                                                                                                                                                                                  |
| App. Acc. Conn. %              | Number of application acceleration connections.                                                                                                                                                                                                                                             |
| HTTP-Comp Rate %               | HTTP compression rate.                                                                                                                                                                                                                                                                      |

**Note**

If any of the percentages that display in the Resource Usage Connections table exceed 100 percent, this is an indication that a license on the ACE was recently installed or uninstalled using either DM or the CLI. To correct the display problem, manually synchronize the Admin context of the ACE with the CLI (see the [“Synchronizing Virtual Context Configurations”](#) section on page 4-79).

**Step 2** Click **Poll Now** to instruct DM to poll the devices and display the current values.

**Step 3** Click **OK** when asked if you want to poll the devices for data now.

**Related Topics**

- [Monitoring Virtual Context Resource Usage, page 14-17](#)
- [Monitoring System Non-Connection Based Resource Usage, page 14-20](#)

## Monitoring System Non-Connection Based Resource Usage

DM displays system-wide, non-connection-based resource usage as explained in the following steps.

**Step 1** Choose **Monitor > Virtual Contexts > System Resource Usage > Features**.

The current resource usage information appears shown in [Table 14-4](#).

**Note**

There might be a slight delay because the resource usage information is gathered real-time.

**Table 14-4** *System Resource Usage Features Field Descriptions*

| Field                              | Description                                             |
|------------------------------------|---------------------------------------------------------|
| Context                            | Name of the virtual context                             |
| Translation Entries %              | Current number of network and port address translations |
| ACL Memory (Bytes) %               | ACL memory usage in bytes                               |
| RegEx Memory (Bytes) %             | Regular expressions memory usage in bytes               |
| Syslog Buffer Size (Bytes) %       | Syslog message buffer size in bytes                     |
| Syslog Message Rate (Messages/S) % | Syslog messages per second                              |

**Step 2** Click **Poll Now** to instruct DM to poll the devices and display the current values.

**Step 3** Click **OK** when asked if you want to poll the devices for data now.

#### Related Topics

- [Monitoring Virtual Context Resource Usage, page 14-17](#)
- [Monitoring System Traffic Resource Usage, page 14-19](#)
- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts, page 14-31](#)

## Monitoring Traffic

DM determines traffic information for your ACE appliance by calculating the delta traffic values since the last polling cycle and displays the resulting values. You can view traffic summary information as provided in the following steps.

#### Procedure

**Step 1** Choose **Monitor > Virtual Contexts > Traffic Summary**.

**Step 2** Use the object selector to view the traffic information for all contexts or a specific context.

The information shown in [Table 14-5](#) appears in the Traffic Summary page.



**Note** You can click on any column heading to sort the table by that column.

**Table 14-5** *Traffic Summary Fields*

| Field     | Description                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------|
| Context   | Name of the context. This field is displayed when the object selector is *All.*                                                   |
| Interface | Name of the interface. Click the interface hyperlink to get traffic data polled directly as shown in <a href="#">Table 14-5</a> . |

Table 14-5 Traffic Summary Fields (continued)

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Status       | User-specified status, which can be one of the following states: <ul style="list-style-type: none"> <li>• Up</li> <li>• Down</li> <li>• Testing, which indicates that no operational packets can be passed.</li> </ul>                                                                                                                                                                                                                                                  |
| Operational Status | Current operational status, which can be one of the following states: <ul style="list-style-type: none"> <li>• Up</li> <li>• Down</li> <li>• Testing, which indicates that no operational packets can be passed</li> <li>• Unknown</li> <li>• Dormant, which indicates the interface is waiting for external actions (such as a serial line waiting for an incoming connection)</li> <li>• Not present, which indicates the interface has missing components</li> </ul> |
| Packets In / Sec   | Per second, the number of packets delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.                                                                                                                                                                                                                                                                                                  |
| Packets Out / Sec  | Per second, the total number of packets that higher-level protocol requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.                                                                                                                                                                                                                                       |
| Bytes In / Sec     | Number of octets received, including framing characters, per second.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Bytes Out / Sec    | Number of octets per second transmitted out of the interface, including framing characters.                                                                                                                                                                                                                                                                                                                                                                             |
| Errors In / Sec    | Number of inbound packets discarded per second because they contained errors or because of an unknown or unsupported protocol.                                                                                                                                                                                                                                                                                                                                          |
| Errors Out / Sec   | Number of outbound packets discarded per second because they contained errors or because of an unknown or unsupported protocol.                                                                                                                                                                                                                                                                                                                                         |
| Last Polled        | Date and time of the last time that DM polled the device to display the current values.                                                                                                                                                                                                                                                                                                                                                                                 |

**Step 3** Click **Poll Now** to instruct DM to poll the ACE and display the current values and click **OK** when prompted if you want to poll the ACE for data now.

**Step 4** Click **Graph** to display a historical trend graph of traffic information (see the “[Configuring Historical Trend and Real Time Graphs for Virtual Contexts](#)” section on page 14-31 for details).

#### Related Topic

- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts, page 14-31](#)



# Monitoring Load Balancing

DM monitors load balancing and allows you to view the information associated with virtual servers, real servers, probes, and load balancing statistics.

This section includes the following topics:

- [Monitoring Load Balancing on Virtual Servers, page 14-23](#)
- [Monitoring Load Balancing on Real Servers, page 14-25](#)
- [Monitoring Load Balancing on Probes, page 14-27](#)
- [Monitoring Load Balancing Statistics, page 14-28](#)

## Monitoring Load Balancing on Virtual Servers

DM monitors load balancing and allows you to display the associated virtual server information as shown in the following steps.



### Note

You can display additional load-balancing information about real servers, such as the number of servers that are functioning properly, and probes, such as viewing if an excessing number of probes are failing, by clicking the hyperlink in the respective columns in [Table 14-6](#).

### Procedure

**Step 1** Choose **Monitor > Virtual Contexts > Load Balancing > Virtual Servers**.

Depending on the virtual context that you selected in the object selector, the information described in [Table 14-6](#) appears.

**Table 14-6** Load Balancing Virtual Server Monitoring Information

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Server           | <p>Name of the virtual server.</p> <p><b>Note</b> If a virtual server is associated with primary and backup server farms, two entries appear in the table: One for the primary server farm and one for the backup server farm.</p> <p>To view statistics for a selected virtual server, click the virtual server hyperlink. The Virtual Server Details popup window appears containing the individual statistic, associated counter value, and a description of the statistic. Click <b>OK</b> to close the popup window.</p> |
| IP Address:Protocol:Port | <p>IP address, protocol and port number of the virtual server. Protocol the virtual server supports, which can be:</p> <ul style="list-style-type: none"> <li>• any—Indicates the virtual server is to accept connections using any IP protocol.</li> <li>• tcp—Indicates that the virtual server is to accept connections that use TCP.</li> <li>• udp—Indicates that the virtual server is to accept connections that use UDP.</li> </ul>                                                                                   |
| Service Policy           | Policy map applied to the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 14-6** Load Balancing Virtual Server Monitoring Information (continued)

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Status        | User-specified status of the virtual server, which can be: <ul style="list-style-type: none"> <li>• In Service—Indicates the server is in service.</li> <li>• Out of Service—Indicates the server is out of service.</li> </ul>                                                                                                                                                                                                                                                                                                                                                 |
| Operational Status  | The state of the server, which can be: <ul style="list-style-type: none"> <li>• Inservice—Indicates the server is in service.</li> <li>• Out of Service—Indicates the server is out of service.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                      |
| DWS                 | Operating state of the Dynamic Workload Scaling feature for the associated server farm, which can be: <ul style="list-style-type: none"> <li>• N/A—Not applicable; the virtual server's server farm is not configured for Dynamic Workload Scaling.</li> <li>• Local—The server farm is configured for Dynamic Workload Scaling, but the ACE is load-balancing traffic to the local VM Controller VMs only.</li> <li>• Expanded—The server farm is configured for Dynamic Workload Scaling and the ACE is sending traffic to the local and remote VM Controller VMs.</li> </ul> |
| Current Connections | Current number of connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Conns/Sec.          | Number of connections per second that the device receives.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Dropped Conns/Sec.  | Number of connections per second that the ACE discarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Server Farm         | Name of the server farm associated with the virtual server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Action              | Indicates if the device is functioning as a primary server (Primary) or a backup server (Backup).                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Algorithm           | Type of predictor algorithm specified on the load balancer, which can be: <ul style="list-style-type: none"> <li>• Roundrobin</li> <li>• Leastconn</li> <li>• Hash URL</li> <li>• Hash Address</li> <li>• Hash Cookie</li> <li>• Hash Header</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| # Rservers Up       | Number of real servers that are up of the real servers configured on the virtual server. For example, when 3 out of 10 real servers are up, 3/10 is displayed.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| # Probes Failed     | Number of probes that have failed of the probes configured on the virtual server. For example, when 10 out of 21 probes fail, 10/21 is displayed.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Last Polled         | Date and time of the last time that DM polled the device to display the current values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Step 2** (Optional) Use the function buttons described in [Table 14-7](#) to update the virtual server information displayed, view graph information, or view the topology map.

**Table 14-7** *Virtual Server Monitoring Window Function Buttons*

| Function Button | Description                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Poll Now</b> | Instructs DM to poll the devices and display the current values. Choose one or more virtual servers and click <b>Poll Now</b> .                                                                                                                                                                                                                       |
| <b>Graph</b>    | Displays a historical trend graph of virtual server information for a specific virtual server. Choose 1 to 4 virtual servers and click <b>Graph</b> .                                                                                                                                                                                                 |
| <b>Topology</b> | Displays the network topology map for a specific virtual server. Choose a virtual server and click <b>Topology</b> .<br><br>The Topology window appears, displaying the virtual server and associated network nodes. For information about using the topology map, see the <a href="#">“Displaying Network Topology Maps” section on page 14-34</a> . |

**Related Topics**

- [Monitoring Load Balancing on Real Servers, page 14-25](#)
- [Monitoring Load Balancing on Probes, page 14-27](#)
- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts, page 14-31](#)

## Monitoring Load Balancing on Real Servers

DM monitors load balancing and allows you to view the associated real server information.

**Procedure**

- Step 1** Choose **Monitor > Virtual Contexts > Load Balancing > Real Servers**.

Depending on the virtual context that you selected from the object selector, the information described in [Table 14-8](#) appears.

**Table 14-8** *Load Balancing Real Server Monitoring Information*

| Field       | Description                                                                                                                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Context     | Name of the context. This field is displayed when the object selector is *All.*                                                                                                                                                                                                                     |
| Real Server | Name of the real server. To view statistics for a selected real server, click the real server hyperlink. The Real Server Details popup window appears containing the individual statistic, associated counter value, and a description of the statistic. Click <b>OK</b> to close the popup window. |
| IP Address  | IP address of the real server. This field appears only for real servers specified as hosts.                                                                                                                                                                                                         |
| Port        | Port number used for the server port address translation (PAT).                                                                                                                                                                                                                                     |
| Server Farm | Primary server farm to use for load balancing.                                                                                                                                                                                                                                                      |

Table 14-8 Load Balancing Real Server Monitoring Information (continued)

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Status       | <p>The specified state of the server, which can be:</p> <ul style="list-style-type: none"> <li>• Inservice—Indicates the server is in service.</li> <li>• Out of Service—Indicates the server is out of service.</li> <li>• In Service Standby—Indicates the server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Operational Status | <p>The state of the server, which can be:</p> <ul style="list-style-type: none"> <li>• Inservice—Indicates the server is in service.</li> <li>• Out of Service—Indicates the server is out of service.</li> <li>• Inservice Standby—Indicates the server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.</li> <li>• Probe Failed—Indicates that DM did not receive a response to a health probe that it sent to the server.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| VM                 | <p>Indicator that the real server is, or is not, a VMware virtual machine as follows:</p> <ul style="list-style-type: none"> <li>• – (dash)—The real server is not a VMware VM.</li> <li>• Yes—The real server is a VMware VM. To view details about the VM, click <b>Yes</b>. The Virtual Machine Details pop-up window appears and provides the following information about the VM: <ul style="list-style-type: none"> <li>– Full path—Full path to the VM.</li> <li>– DNS Name—DNS name of the VM.</li> <li>– IP Address—VM IP address.</li> <li>– State—Operating state of the VM (for example, poweredOn).</li> <li>– Guest OS—Guest operating system (for example, Red Hat Enterprise Linux 5 (32-bit)).</li> <li>– Host—Host IP address.</li> <li>– Memory (MB)—Amount of memory.</li> <li>– CPU (MHz)—CPU frequency.</li> <li>– Triggered Alarms—Number of recorded triggered alarm conditions.</li> </ul> </li> </ul> <p>Click <b>OK</b> to close the Virtual Machine Details pop-up window.</p> |
| Weight             | Weight assigned to the real server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Locality           | <p>Locality also requires that you have the ACE configured for Dynamic Workload Scaling (see the “<a href="#">Configuring Dynamic Workload Scaling</a>” section on page 6-14).</p> <p>Possible values for real server locality are as follows:</p> <ul style="list-style-type: none"> <li>• N/A—Not available; the ACE cannot determine the real server location (local or remote). A possible cause for this issue is that Dynamic Workload Scaling is not configured correctly.</li> <li>• Local—The real server is located in the local network.</li> <li>• Remote—The real server is located in the remote network. The ACE bursts traffic to this server when the local real server's CPU and/or memory usage reaches the specified maximum threshold value.</li> </ul>                                                                                                                                                                                                                              |

Table 14-8 Load Balancing Real Server Monitoring Information (continued)

| Field             | Description                                                                                                                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Current Conns     | Number of current connections to this server. If this field indicates <i>N/A</i> , the database does not have any information about current connections. If this field is 0, the database received an SNMP response of 0. |
| Conns/Sec         | Connections per second.                                                                                                                                                                                                   |
| Dropped Conns/Sec | Dropped connections per second.                                                                                                                                                                                           |
| Last Polled       | Date and time of the last time that DM polled the device to display the current values.                                                                                                                                   |

**Step 2** (Optional) Use the function buttons described in [Table 14-9](#) to update or change the real server information displayed.

Table 14-9 Real Server Monitoring Window Function Buttons

| Function Button | Description                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Poll Now</b> | Instructs DM to poll the devices and display the current values. Choose one or more real servers and click <b>Poll Now</b> . Click <b>OK</b> when asked if you want to poll the devices for data now.                                                                                                                                                              |
| <b>Graph</b>    | Displays a historical trend graph of real server information for the specified real servers. Choose 1 to 4 real servers and click <b>Graph</b> . Choosing multiple real servers allows you to compare information. For more information, see the “ <a href="#">Configuring Historical Trend and Real Time Graphs for Virtual Contexts</a> ” section on page 14-31. |
| <b>Topology</b> | Displays the network topology map for the specified real server. Choose a real server and click <b>Topology</b> .<br>The Topology window appears, displaying the real server and associated network nodes. For information about using the topology map, see the “ <a href="#">Displaying Network Topology Maps</a> ” section on page 14-34.                       |

#### Related Topics

- [Monitoring Load Balancing](#), page 14-23
- [Monitoring Load Balancing on Probes](#), page 14-27
- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts](#), page 14-31

## Monitoring Load Balancing on Probes

To check the health and availability of a real server, the ACE periodically sends a probe to the real server. If you notice an excessive number of probes failing, you can view the monitoring information as shown in the following steps.

#### Procedure

**Step 1** Choose **Monitor > Virtual Contexts > Load Balancing > Probes**.

Depending on the virtual context that you selected from the object selector, the probe information described in [Table 14-10](#) appears.

**Table 14-10** *Load Balancing Probes Monitoring Information*

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Context             | Name of the context. This field is displayed when the object selector is *All.*                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Probe               | <p>Name of the probe.</p> <p>To view statistics for a selected probe, click the probe hyperlink. The Probe Details popup window appears containing the following probe statistics:</p> <ul style="list-style-type: none"> <li>Failed Probes—Total number of failed probes.</li> <li>Health of Probes—Health of the probe. Possible values are PASSED or FAILED.</li> <li>Probes Passed—Total number of passed probes.</li> </ul> <p>Click <b>OK</b> to close the Probe Details popup window.</p> |
| Type                | Type of probe. For a complete list of probe types and their descriptions, see <a href="#">Table 6-9</a> .                                                                                                                                                                                                                                                                                                                                                                                        |
| Real Server         | Name of the real server that the probe is associated with.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Farm         | Name of the server farm that the probe is associated with.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Port                | Port number that the probe uses. By default, the probe uses the port number based on its type.                                                                                                                                                                                                                                                                                                                                                                                                   |
| IP Address of Probe | Destination or source address for the probe.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Probed Port         | Source of the probe port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Probe Health        | Health of the probe. Possible values are PASSED or FAILED.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Passed Rate         | Rate of passed probes                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Failed Rate         | Rate of failed probes                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Last Polled         | Date and time of the last time that DM polled the device to display the current values.                                                                                                                                                                                                                                                                                                                                                                                                          |

**Step 2** Click **Poll Now** to instruct DM to poll the devices and display the current values.

**Step 3** Click **OK** when asked if you want to poll the devices for data now.

#### Related Topics

- [Monitoring Load Balancing, page 14-23](#)
- [Monitoring Load Balancing Statistics, page 14-28](#)
- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts, page 14-31](#)

## Monitoring Load Balancing Statistics

You can monitor load balancing on your ACE as shown in the following procedure.

#### Procedure

**Step 1** Choose **Monitor > Virtual Contexts > Load Balancing > Statistics**.

Depending on the virtual context that you selected from the object selector, the Load Balancing Statistics Monitoring Information window displays the information described in [Table 14-11](#).

**Table 14-11** Load Balancing Statistics Monitoring Information

| Field                                     | Description                                                                             |
|-------------------------------------------|-----------------------------------------------------------------------------------------|
| Context                                   | Name of the context. This field is displayed when the object selector is *All.*         |
| L4 Policy Conn                            | Number of Layer 4 policy connections.                                                   |
| L7 Policy Conn                            | Number of Layer 7 policy connections.                                                   |
| Failed Conn                               | Number of failed connections.                                                           |
| Dropped L4 Policy Conn                    | Number of dropped Layer 4 policy connections.                                           |
| Dropped L7 Policy Conn                    | Number of dropped Layer 7 policy connections.                                           |
| Rejected Conn Due To No Policy Match      | Number of connections rejected because they did not match policies.                     |
| Rejected Conn Due To No Configured Policy | Number of connections rejected because there are no configured policy.                  |
| Rejected Conn Due To ACL Deny             | Number of connections rejected due to ACL parameters.                                   |
| Rejected Conn Due To L7 Config Changes    | Number of rejected connections due to Layer 7 configuration changes.                    |
| Conn Timed Out                            | Number of times the connection timed out.                                               |
| Last Polled                               | Date and time of the last time that DM polled the device to display the current values. |

- Step 2** Click **Poll Now** to instruct DM to poll the devices and display the current values and click **OK** when prompted if you want to poll the devices for data now.
- Step 3** Click **Graph** to display a historical trend graph of load balancing statistics (see the “[Configuring Historical Trend and Real Time Graphs for Virtual Contexts](#)” section on page 14-31 for details).

#### Related Topic

- [Monitoring Load Balancing on Probes, page 14-27](#)
- [Configuring Historical Trend and Real Time Graphs for Virtual Contexts, page 14-31](#)

## Monitoring Application Acceleration

If you have configured application acceleration functions on the ACE, you can monitor the optimization statistics as shown in the following steps.

- Step 1** Choose **Monitor > Virtual Contexts > Application Acceleration**.
- Depending on the virtual context that you selected from the object selector, the Application Acceleration information appears as shown in [Table 14-12](#).

**Note**

For connection-based syslogs, the following additional parameters are displayed: Source IP, Source Port, Destination IP, Destination Port, and Protocol Information. This allows you to sort and filter on these fields if desired.

**Table 14-12**      *Application Acceleration Monitoring View*

| Field                            | Statistic                                  | Description                                                                                                |
|----------------------------------|--------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Condenser Information            | Total HTTP Unoptimized Requests Received   | Total number of end-user HTTP request the condenser has received that cannot be optimized                  |
|                                  | Accumulated Bytes Received                 | Accumulated size (in bytes) of each end-user requested object                                              |
|                                  | Total Responses in Bytes                   | Accumulated size (in bytes) of responses, both for condensable and non-condensable end-user HTTP requests  |
|                                  | Total Abandons of Delta Optimization       | Total number of abandons of delta optimization requests                                                    |
| Cacheable Objects Statistics     | Total Objects Served from Cache            | Total number of cacheable objects served from the cache, excluding the not-modified replies                |
|                                  | Accumulated Bytes Served                   | Accumulated size (in bytes) of the cacheable objects served from the cache, excluding not-modified replies |
|                                  | Total Objects Not Found in Cache           | Total number of cacheable objects not found in the cache                                                   |
|                                  | Accumulated Bytes Not Found                | Accumulated size (in bytes) of the cacheable objects not found in the cache                                |
|                                  | Total IMS Requests for Valid Cache         | Total number of IMS requests for valid copies of objects in the cache                                      |
|                                  | Total Missed IMS Requests                  | Total number of IMS request for objects that either do not exist or are stale in the cache                 |
|                                  | Total Non-Cacheable Object Requests        | Total number of non-cacheable object requests                                                              |
|                                  | Total Requests with Not Modified Responses | Total number of requests for stale objects that have the response from the origin server as not modified   |
| Flash Forward Objects Statistics | Successful Transformations                 | Total number of successful transformations for FlashForward objects                                        |
|                                  | Unsuccessful Transformations               | Total number of unsuccessful transformations for FlashForward objects                                      |
|                                  | Total HTTP Requests                        | Total number of HTTP requests (excluding the IMS requests) for the transformed FlashForward objects        |
|                                  | Total IMS Requests                         | Total number of IMS requests for transformed FlashForward objects                                          |

**Step 2**      Click **Poll Now** to instruct DM to poll the devices and display the current values.

**Step 3**      Click **OK** when asked if you want to poll the devices for data now.



**Related Topic**

[Configuring Application Acceleration and Optimization, page 13-1](#)

# Configuring Historical Trend and Real Time Graphs for Virtual Contexts

DM allows you to store historical data for a selected list of statistics calculated over the last hour, 2-hour, 4-hour, 8-hour, 24-hour, or month interval. You can view this historical data as a statistical graph from specific Monitor > Virtual Contexts monitoring screens. For each monitoring page, default statistics are defined and the graph drawn for the selected object(s) from the page. DM also allows you to display real time statistical information related to the selected monitoring window.

**Note**

All client browsers require that you enable Adobe Flash Player 9 to properly display the monitoring graphs provided in DM.

Historical graphs are available from the following Monitor > Virtual Contexts monitoring windows:

- Traffic Summary window
- Load Balancing > Virtual Server window
- Load Balancing > Real Server window
- Load Balancing > Statistics window
- Context Resource Usage

In each monitoring view window, click the **Graph** button to view the Graph page. From this page you can view up to a maximum of four individual graphs of object data. Tooltips appears within each graph to allow you to see the datapoint values used for plotting.

If you choose, you can overlay multiple objects for comparison on the same graph. Each graph grid provide a comma-separated list of select statistics.

DM supports a maximum of four lines per historical graph. The number of lines in a graph indicates the number of combinations of statistics and the objects (which can be a virtual server, real server, virtual context, and so on). For example, if you select two statistics and two real servers, then the number of possible combination that can be displayed in a graph is four.

**Note**

The time displayed in all graphs is shown in DM server time not in client time.

**Procedure**

- Step 1** Choose the specific monitoring window from which you want to display historical data graphs for a selected list of items.

**Table 14-13**      *Selecting a Monitoring Window*

| To Access....          | Select...                                                        |
|------------------------|------------------------------------------------------------------|
| Resource Usage window  | <b>Monitor &gt; Virutal Contexts &gt; Context Resource Usage</b> |
| Traffic Summary window | <b>Monitor &gt; Virutal Contexts &gt; Traffic Summary</b>        |

Table 14-13 Selecting a Monitoring Window

| To Access....          | Select...                                                                     |
|------------------------|-------------------------------------------------------------------------------|
| Virtual Servers window | <b>Monitor &gt; Virutal Contexts &gt; Load Balancing &gt; Virtual Servers</b> |
| Real Servers window    | <b>Monitor &gt; Virutal Contexts &gt; Load Balancing &gt; Real Servers</b>    |
| Statistics window      | <b>Monitor &gt; Virutal Contexts &gt; Load Balancing &gt; Statistics</b>      |

- Step 2** Check the check box of the objects in the selected monitoring window that you want to view and click **Graph**.

The graph window appears.

DM supports a maximum selection of up to four objects. DM updates the monitoring window with the graph of the selected objects.

At any point, if you want to add a graph to the selected monitoring window, click **Add Graph**.



**Note** DM supports a maximum of four objects that you can select in a specific Monitor > Virtual Contexts monitoring window.

- Step 3** To enhance your viewing of the graphs, use the Collapse/Expand buttons to minimize or maximize a graph in the monitoring window.

- Step 4** To toggle the display of an object graph in the monitoring window, do the following:

- Click **View As Chart** to display the object data as a graph.
- Click **View As Grid** to display the object data as a numerical line grid.



**Note** If you want to save the graph as a JPEG file for archive or other purposes, click the **Show As Image** button. When you mouse over the graph, the Image Toolbar appears. From the Image Toolbar, you can save the graph as a JPEG or send it in an email. You can also print the graph if desired.

If you want to export object data to Microsoft Excel for archive or other purposes, click the **Export to Excel** link in the View As Grid object display.

- Step 5** To add one or more objects to a graph in the monitoring window to compare the performance of one object with its peer for the selected stats, do the following:

- In the Selected {Object} line in the graph of the object that you want to replace, click the **Select** button.

The Objects Selector pop-up window appears.

- From the Objects Selector pop-up window, choose a different object and click **OK**.

The selected object replaces the existing object graph in the monitoring window.



**Note** DM supports a maximum of four lines to be drawn per historical graph.

- Step 6** To select multiple statistics for display in a graph in the monitoring window, perform the following steps:
- In the Selected Stat(s) line in the graph of the object that you want to add statistics, click the **Select** button within the graph.  
The Select Stats pop-up window appears.
  - From the Select Stats pop-up window, choose one or more statistics to add to the graph and click **OK**.  
You can choose up to four statistics for display in a graph and the object statistics must be of the same unit of measure (for example, bytes/sec.). The selected statistics appear in the existing object graph in the monitoring window.
- Step 7** To modify the time interval for the accumulated statistics displayed in a graph, click the **Time** drop-down list to display the list of time interval options.
- Time interval choices include the average data calculated during the last hour, 2-hour, 4-hour, 8-hour, 24-hour, or 30-day (last month) interval. The time choices also include the Real Time option, which at most displays 3 minutes of data at 10 second intervals (not configurable).
- Note the following usage considerations for the time interval for accumulated statistics:
- When you specify to view average data calculated during the last hour, 2-hour, 4-hour, or 8-hour interval, raw data points collected by DM within the selected time period will be displayed. For example, in the case of the last 1 hour, if DM has been collecting data for over an hour at a default 5-minute interval, you will see 12 data points on the graph.
  - When you specify to view average data calculated during the last 24-hour interval, consolidated hourly data points will be displayed. For example, if DM has been collecting data for more than 24 hours, you will see 24 data points on the graph.
  - When you specify to view average data calculated during the last 30-day interval, consolidated daily data points will be displayed. For example, if DM has been collecting data for over 30 days, you will see 30 data points on the graph.
- Step 8** To exit the display of graphs, click **Exit Graph**.
- 

## Setting Up Virtual Contexts Statistics Collection

Use the procedure to enable data collection for the virtual contexts you select. Configuration changes are not saved after an appliance reboot; default settings are restored.

For more information about ACE appliance hardware statistics such as CPU, disk, and memory usage, see [Monitoring ACE Appliance Statistics, page 15-35](#).

### Procedure

- 
- Step 1** Select **Monitor > Virtual Contexts > Statistics Collection**. Depending on the virtual context that you selected from the object selector, the Statistics Collection screen appears.
- Step 2** In the Polling Stats field, select **Enable** to start background polling or **Disable** to stop background polling.
- Step 3** In the Background Polling Interval field, select the polling interval appropriate for your networking environment. The interval range is from one minute to six hours.
- Step 4** Click **Deploy Now** to save your entries.



**Note** These settings are not saved if you reboot your appliance. The system defaults will be restored.

#### Related Topics

- [Control Plane CPU/Memory Graphs, page 14-10](#)
- [Monitoring Load Balancing on Real Servers, page 14-25](#)
- [Monitoring Load Balancing on Probes, page 14-27](#)

## Displaying Network Topology Maps

This section shows how to display and use the network topology maps that display the nodes on your network based on the virtual or real server that you select.

**Table 14-14**      *Network Topology Map Components*

| Component             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Topology map tool bar | <p>Located above the topology map, the tool bar contains the following tools:</p> <ul style="list-style-type: none"> <li>• <b>Layout</b>—Changes the direction in which the network map appears. Choose one of the following options from the drop-down list: Top to Bottom or Left to Right.</li> <li>• <b>Zoom</b>—Modifies the size of the network map. Click and drag the slide bar pointer to adjust the map size.</li> <li>• <b>Magnifier</b>—Toggle button that enables or disables the magnifier tool. When enabled, moving your mouse over the the topology map magnifies the area that the mouse is over.</li> <li>• <b>Fit Content</b>—Fits the topology map to the window.</li> <li>• <b>Overview</b>—Toggle button that enables or disables the Overview Window tool (see <a href="#">Overview Window</a>).</li> <li>• <b>Undo</b>—Sets the network node icons back to their previous positions.</li> <li>• <b>Redo</b>—Redoes the changes that you made before you clicked Undo.</li> <li>• <b>Print</b>—Sends the topology map to the network printer.</li> <li>• <b>Exit</b>—Closes the topology map and returns to the previous window.</li> </ul> |

Table 14-14 Network Topology Map Components (continued)

| Component       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Topology Map    | <p>Displays network node mapping.</p> <p>The node icons display the following information related to the node:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• IP address (virtual and real servers only)</li> <li>• Port (real servers only)</li> <li>• Operational state (virtual and real servers only)</li> </ul> <p>When you hover over a network node icon, the node type appears, for example ACE Virtual Server, Server Farm, or Real Server. Other possible operations when you hover over a network node icon are as follows:</p> <ul style="list-style-type: none"> <li>• Real servers only—When you have an ACE configured for Dynamic Workload Scaling and you mouseover an associated real server icon, information appears that identifies which data center the real server is located in: local or remote. A timestamp also appears that specifies when the information was obtained.</li> <li>• Server farms only—When you mouseover a server farm icon, the following Dynamic Workload Scaling status information appears: <ul style="list-style-type: none"> <li>– Local—The ACE is using the server farm’s local real servers only for load balancing. A timestamp specifies when the information was obtained.</li> <li>– Burst—The ACE is bursting traffic to the server farm’s remote real servers because the load of the local real servers has exceeded the specified usage threshold (based on the average CPU and/or memory usage). A timestamp specifies when the information was obtained.</li> <li>– N/A—Not applicable (Dynamic Workload Scaling is not available).</li> </ul> </li> </ul> <p>For more information about Dynamic Workload Scaling, see the <a href="#">“Dynamic Workload Scaling Overview” section on page 6-4</a>.</p> <p>To view details about a network node, right-click on the node and choose <b>Show Details</b> from the pop-up menu. To reposition a node in the map, click and drag the node icon to a new position. The node interconnect lines move with the node.</p> |
| Overview Window | <p>Provides a combined functionality of the scroll bars and zoom tool as follows:</p> <ul style="list-style-type: none"> <li>• Position tool (a)—Click and drag the shaded box to move around the topology map.</li> <li>• Zoom tool (b)—Click and drag the shaded box handle (located in lower right corner) and to zoom in or out of the topology map.</li> </ul> <p>Click the Overview toggle button in the map tool bar to display or hide the Overview window (see <a href="#">Topology map tool bar</a>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

### Procedure

- Step 1** Do one of the following:
- Display the list of virtual servers by choosing **Monitor > Virtual Contexts > Loadbalancing > Virtual Servers**.
- The Virtual Servers window appears with the table of configured virtual servers.

- Display the list of real servers, choose **Monitor > Virtual Contexts > Loadbalancing > Real Servers**.

The Real Servers window appears with the table of configured virtual servers.

**Step 2** From the servers table, check the check box next to the server whose topology map you want to display.

**Step 3** From the servers window, click **Topology**.

The DM Topology window displays the topology map for the selected virtual or real server. For information about using the topology map tools, see [Table 14-14](#).

**Step 4** (Optional) To close the topology map and return to the previous window, from the DM Topology window, click **Exit**.

## Testing Ping

Use the following steps to verify the **ping** command on a device.

### Procedure

**Step 1** Select **Monitor > Virtual Contexts > context > Ping**.

**Step 2** Enter the information shown in [Table 14-15](#).

**Table 14-15** Ping Fields

| Field           | Description                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------|
| IP Address Type | Select either IPv4 or IPv6 for the address type of the real server.                                        |
| IP Address      | Enter the IP address of the real server to which you want to ping.                                         |
| Elapsed Time    | Elapsed time before the ping request is declared a failure.                                                |
| Repeat          | Enter how many times to repeat the test.                                                                   |
| Datagram Size   | Enter a value for the argument size (size of the packet) of the ping command. Range is between 36 and 452. |

**Step 3** Click **Start** to run the connectivity test.

If ping fails, it may take up to 30 seconds before an error is returned. A future release will have a Cancel button.

**Step 4** After the test completes, the results are displayed. Do the following:

- Click **New** to enter new parameters and create a new ping test. After selecting New, the Start New Test page displays. You may click Results if you want to review the results of the test you just performed.
- Click **Restart** to rerun the connectivity test.

### Related Topics

- [Setting Up Virtual Contexts Statistics Collection, page 14-33](#)

- [Monitoring Load Balancing on Real Servers, page 14-25](#)
- [Monitoring Load Balancing on Probes, page 14-27](#)







# CHAPTER 15

## Managing the ACE Appliance

---

The following sections describe how to manage the ACE appliance using ACE Appliance Device Manager:

- [Overview of the Admin Functions, page 15-1](#)
- [Controlling Access to the Cisco ACE Appliance, page 15-3](#)
- [Managing Users, page 15-7](#)
- [Managing User Roles, page 15-14](#)
- [Managing Domains, page 15-31](#)
- [Monitoring ACE Appliance Statistics, page 15-35](#)
- [Using Admin Tools, page 15-37](#)

For details on logging into ACE Appliance Device Manager, see [Logging into ACE Appliance Device Manager, page 1-4](#).



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

## Overview of the Admin Functions

Use the Admin tab to manage role-based access control, set up and view statistical data for the ACE appliance, and use troubleshooting tools for the ACE Appliance Device Manager.



### Note

Some of the Admin options might not be visible to some users; the roles assigned to your login determine which options are available.

---

Table 15-1 describes the options that are displayed when you click **Admin**.

**Table 15-1** Admin Menu Options

| Menu                      | Option       | Description                                                                                                                                                                                                                                  | Reference                                                                                                                     |
|---------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Role-Based Access Control | Users        | Manage users and their access to their context                                                                                                                                                                                               | See <a href="#">Managing Users</a> , page 15-7                                                                                |
|                           | Active Users | Display or end session for active users                                                                                                                                                                                                      | See <a href="#">Displaying Current User Sessions</a> , page 15-11 or <a href="#">Ending Active User Sessions</a> , page 15-12 |
|                           | Roles        | Manage user's access to commands and resources                                                                                                                                                                                               | See <a href="#">Managing User Roles</a> , page 15-14                                                                          |
|                           | Domains      | Manage an association between a select group of context users and a select group of context objects.                                                                                                                                         | See <a href="#">Managing Domains</a> , page 15-31                                                                             |
| Device Management         |              | Check the status of the ACE Appliance Device Manager                                                                                                                                                                                         | See <a href="#">Monitoring ACE Appliance Statistics</a> , page 15-35                                                          |
| Tools                     |              | Report a problem to the Cisco support line and generate a diagnostic package, access files from the ACE appliance for viewing or tracking, and replace all virtual context configurations with the CLI configurations from the ACE appliance | See <a href="#">Using ACE Appliance Device Manager Troubleshooting Tools</a> , page 16-1                                      |

#### Related Topics

- [Managing the ACE Appliance](#), page 15-1
- [Controlling Access to the Cisco ACE Appliance](#), page 15-3

# Controlling Access to the Cisco ACE Appliance

Access to ACE Appliance Device Manager is controlled using the same username and password that access the ACE appliance. This enables authentication to a local database or to an external RADIUS, TACACS+, or LDAP server. If you choose to authenticate using AAA and not the local database, you must configure AAA using the CLI. For details on setting up remote authentication using AAA servers, see the *Security Guide, Cisco ACE Application Control Engine*.

**Note**

The ACE supports local user authentication using a local database on the ACE or through remote authentication using one or more AAA servers. AAA remote servers are grouped into independent groups of TACACS+, RADIUS, or LDAP servers. Authentication allows you to control user access to the ACE by requiring specification of a valid username and password, or no password verification. When you configure the ACE appliance from the CLI to support the user authentication and accounting functions, the Device Manager honors the tasks that are performed by the specified remote server. See the *Security Guide, Cisco ACE Application Control Engine* for details about authentication and accounting.

In addition, the role and domains that a user is associated with on a remote server will also be honored by the Device Manager.

The ACE Appliance Device Manager does not configure AAA; instead, it uses role-based access control for access to features. When a user logs into the system, the specific tasks they can perform and areas of the system they can use are controlled by *contexts*, *roles*, and *domains*. If you need to restrict a user's access, you must first assign a role-domain pair.

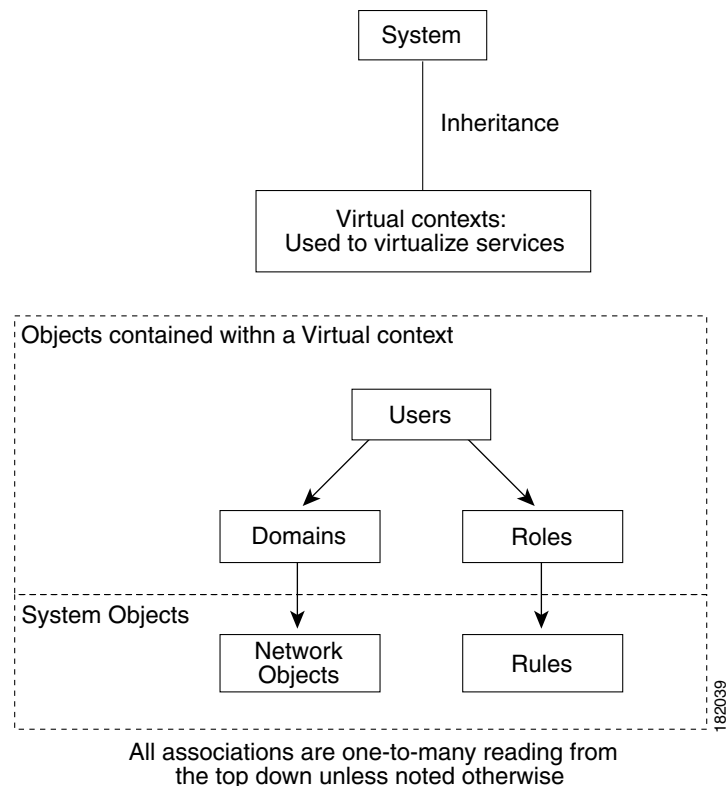
The role assigned to a user defines the tasks a user can perform and the items in the hierarchy that they can see. Roles are either predefined or set up by the system administrator. Each role, user, and domain is associated with a context. Only roles and domains associated with the Admin context can see other contexts. See [Understanding Roles, page 15-5](#) for more information.

A domain is a collection of managed objects. When a user is given access to a domain, this acts as a filter for a subset of objects on the network which are displayed as a virtual context. The types of objects in the system that are domain controlled are as follows:

- All objects listed below
- Access list—Ethertype
- Access list—Extended
- Class-map
- Interface VLAN
- Interface BVI
- Parameter-map
- Policy-map
- Probe
- Real server
- Script
- Server farm
- Sticky

Thus, role-based access control ensures that users can view only the devices or services or perform the actions that are included in the domains to which they have been given access.

**Figure 15-1** Role-Based Access Control Containment Overview



The following is an example of role-based access control containment.

| Domains                                      |                 |                    |
|----------------------------------------------|-----------------|--------------------|
| East Coast servers                           | Central servers | West Coast servers |
| Role                                         |                 |                    |
| Web server administrator                     |                 |                    |
| Users                                        |                 |                    |
| User A                                       | User B          | User C             |
| <b>Note</b> Each association is one-to-many. |                 |                    |

All other user interfaces, such as configuration, monitoring, and administration, respect this role-based access control policy:

- Roles limit the screens (or functions on those screens) that a user can see.
- Domains limit the objects that are listed on any screen that the roles allow.
- Users (other than the administrator) can create only subdomains of the domains to which they are assigned. However, no parent/child relationship is kept between domains.
- The system administrator user (Admin) can see and modify all objects. All other users are subject to the role-based access controls illustrated in [Figure 15-1](#).

**Related Topics**

- [Types of Users, page 15-5](#)
- [Understanding Roles, page 15-5](#)
- [Understanding Operations Privileges, page 15-6](#)
- [Understanding Domains, page 15-7](#)
- [Managing Users, page 15-7](#)

## Types of Users

Two types of users configure and monitor the ACE appliance:

- **Default user**—Individuals associated with the data center or IT department where the ACE appliance is installed. The default administrative account (user ID **admin**) is a system user account that is preconfigured on the system. The admin user password is previously set when the system was installed. You can change the password for the admin user account in the same manner as any user password (see [Managing Users, page 15-7](#)).

Predefined system roles are specified in terms of roles, domains, and operations privileges. Each role can work with a specific set of operations and domains in a context.

- **Assigned users**—Users to whom you want to grant access to ACE appliance. You can assign users limited access by selecting roles and domains to which they belong. Users are not allowed to change to other contexts and can work with a specific set of operations and domains in the context in which they were created.

**Related Topics**

- [Managing Users, page 15-7](#)
- [Guidelines for Managing Users, page 15-8](#)
- [Displaying a List of Users, page 15-8](#)
- [Creating User Accounts, page 15-8](#)

## Understanding Roles

User roles determine the privileges that a user has, the features they can access, and the actions they can take in a particular context.

Cisco ACE appliance provides a set of predefined roles (see [Table 15-2 on page 15-9](#)). Additional roles can also be defined by the system administrator. Roles are specified in terms of resource types and operations privileges known as rules. For each role, rules provide permissions about which resource types a role can work with and what operations a role can perform on each resource type.

Each user is assigned one role (Network-Monitor is the default) and inherit the operations privileges specified for each of the rules assigned to that role. Users are assigned one role. Each role can have different access privileges (in the form of rules) that are independent of other assigned roles.

The options a user sees in the menu are filtered according to that user's role.

**Note**

If you need to restrict a user's access, you must assign a role-domain pair. Otherwise, no matter what roles the user may have, that user will not be able to access any specific resources, and, therefore, will have no powers on the system.

All users are strictly limited by the combination of their contexts, roles, and domains. For example, a user cannot create another user who has greater privileges or access or is outside their domain.

Roles cannot be deleted if they are currently referenced by a user. The predefined roles cannot be changed or deleted.

**Related Topics**

- [Guidelines for Managing User Roles, page 15-14](#)
- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)
- [Displaying User Roles, page 15-28](#)
- [Creating User Roles, page 15-28](#)
- [Modifying User Roles, page 15-30](#)
- [Deleting User Roles, page 15-30](#)

## Understanding Operations Privileges

Operations privileges define what users can do in the designated context. There are two levels of access. The first level is the permit or deny permission. The second level is the operations privilege the user is permitted or denied from performing. For example, each feature on the ACE appliance has an assigned privilege. If a user's privileges are not sufficient, the feature will not be available to them. The following operations privileges can be permitted or denied from least to greatest privilege levels:

- Monitor—Allows the user to view statistics and specify parameter collection.
- Modify—Allows the user to change the persistent information associated with system objects, such as a configuration.
- Debug—Allows the user to collect information on existing problems.
- Create—Allows the user to control system objects, for example, creating them, enabling them, or powering up; also has delete permission.

Privileges are hierarchical. If a user has Modify privileges, they have Monitor privileges as well. If a user has Create or Debug privileges, they have Modify privileges as well. Only Admin has Resource Class Mgmt access.

**Note**

The ability to create automatically contains the modify function, but the reverse is not true (a user with modify privileges cannot automatically create items).

**Related Topics**

- [Guidelines for Managing User Roles, page 15-14](#)
- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)
- [Managing User Roles, page 15-14](#)

## Understanding Domains

Cisco ACE appliance provides a predefined default domain that contains all objects. You cannot modify or delete the predefined domain. Additional domains can be defined by the system administrator. A domain is a collection of managed objects to which a user is given access. By setting up a customized domain, you are filtering a subset of objects on the network. The user is then given access to this domain.

For example, a user can see only what is in the domain to which they have access (achieved through row filtering). If the default domain contains 50 objects and the customized domain, dom1, consists of the following domain objects: Rserver rs1, Rserver rs2, Serverfarm sf1, Serverfarm sf2, and Accesslist extended acl1, a user associated with domain dom1, can see only those five objects within the whole context.

The rows a user sees in any table are filtered according to the domain to which that user has access.



**Note** If you need to restrict a user's access, you must assign a role-domain pair. Otherwise, no matter what roles the user may have, that user will not be able to access any specific resources, and, therefore, will have no powers on the system.

### Related Topics

- [Managing Domains, page 15-31](#)
- [Guidelines for Managing Domains, page 15-31](#)

## Managing Users

Use the Role-Based Access Control feature to specify the people that are allowed to log onto the system. The following sections describe how to manage user accounts:

- [Guidelines for Managing Users, page 15-8](#)
- [Displaying a List of Users, page 15-8](#)
- [Creating User Accounts, page 15-8](#)
- [Modifying User Accounts, page 15-10](#)
- [Deleting User Accounts, page 15-10](#)
- [Displaying Current User Sessions, page 15-11](#)



**Note**

The ACE supports local user authentication using a local database on the ACE or through remote authentication using one or more AAA servers. AAA remote servers are grouped into independent groups of TACACS+, RADIUS, or LDAP servers. Authentication allows you to control user access to the ACE by requiring specification of a valid username and password, or no password verification. When you configure the ACE appliance from the CLI to support the user authentication and accounting functions, the Device Manager honors the tasks that are performed by the specified remote server. See the *Security Guide, Cisco ACE Application Control Engine* for details about authentication and accounting.

In addition, the role and domains that a user is associated with on a remote server will also be honored by the Device Manager.

## Guidelines for Managing Users

- For users that you create in the Admin context, the default scope of access is for the entire ACE.
- If you do not assign a role to a new user, the default user role is Network-Monitor. For users that you create in other contexts, the default scope of access is the entire context.
- Users cannot log in until they are associated with a domain and a user role.
- You cannot delete roles and domains that are associated with an existing user.

## Displaying a List of Users

### Procedure

- 
- Step 1** Select **Admin > Role-Based Access Control > Users**. The Users table appears with the following fields:
- Name
  - Expiry Date
  - Role
  - Domains
- Step 2** You can use the options in this screen to create a new user or modify or delete any existing user to which you have access (see [Table 15-2](#)).
- 

### Related Topics

- [Creating User Accounts, page 15-8](#)
- [Deleting User Accounts, page 15-10](#)
- [Managing Users, page 15-7](#)
- [Guidelines for Managing Users, page 15-8](#)

## Creating User Accounts



### Note

---

Your user role determines whether you can use this option.

---



### Procedure

- 
- Step 1** Select **Admin > Role-Based Access Control > Users**. A list of users appears in the Users table.
- Step 2** Click **Add**.



**Step 3** Complete the following required fields (unless otherwise noted):

**Table 15-2** *User Attributes*

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                     | Specifies the name by which the user is to be identified in the system (up to 24 characters). Only letters, numbers, and underscore can be used. The field is case sensitive.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Expiry Date <sup>1</sup> | Date the user name is usable in the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Password Entered As      | Specifies whether the password is entered as Clear Text or Encrypted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Password                 | Allows you to specify a password for this user account. Password must be at least 8 characters long.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Confirm                  | Ensures password is keyed in properly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Role                     | <p>Specifies the definition of what a user can do in this system. Choose from the following options or create your own role:</p> <ul style="list-style-type: none"> <li>• Admin</li> <li>• Network-Admin</li> <li>• Network-Monitor</li> <li>• Security-Admin</li> <li>• Server-Appln-Maintenance</li> <li>• Server-Maintenance</li> <li>• SLB-Admin</li> <li>• SSL-Admin</li> </ul> <div>  <p><b>Note</b> The SSL-Admin role is not available with the ACE NPE software version (see the <a href="#">“Information About the ACE No Payload Encryption Software Version”</a> section on page 1-2).</p> </div> <div>  <p><b>Note</b> If you need to restrict a user’s access, you must assign a role-domain pair.</p> </div> <p>See <a href="#">Table 15-4 on page 15-15</a> for details about predefined roles.</p> |
| Domains                  | A means for organizing the devices and their components (physical and logical) in your network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

1. Not required.

**Step 4** Click **Deploy Now** to deploy this configuration. The Users table reappears.

**Step 5** To add another user, click **Add Another**.

#### Related Topics

- [Modifying User Accounts, page 15-10](#)

- [Deleting User Accounts, page 15-10](#)
- [Displaying a List of Users, page 15-8](#)
- [Managing Users, page 15-7](#)
- [Guidelines for Managing Users, page 15-8](#)

## Modifying User Accounts



### Note

Your user role determines whether you can use this option.

### Procedure

- Step 1** Select **Admin > Role-Based Access Control > Users**. The Users table appears.
- Step 2** Select the user account you want to modify.
- Step 3** Click **Edit**.
- Step 4** The User details screen appears. Make any changes (see [Table 15-2](#)) and click **Deploy Now**. The Users table then appears.

### Related Topics

- [Creating User Accounts, page 15-8](#)
- [Deleting User Accounts, page 15-10](#)
- [Displaying a List of Users, page 15-8](#)
- [Managing Users, page 15-7](#)
- [Guidelines for Managing Users, page 15-8](#)

## Deleting User Accounts

You can delete users using this procedure. You can also delete users from the Active Users window.



### Note

Your user role determines whether you can use this option.

### Procedure

- Step 1** Select **Admin > Role-Based Access Control > Users**. The Users table containing user, role, domain and other user information appears.
- Step 2** Select the user account to be deleted.
- Step 3** Click **Delete**.  
A window appears asking you to confirm the deletion.

- Step 4** Click **OK** to delete the user account or **Cancel** to exit the procedure without deleting the user. If you click OK, the window refreshes with the Users table and the deleted user account no longer appears.

#### Related Topics

- [Creating User Accounts, page 15-8](#)
- [Modifying User Accounts, page 15-10](#)
- [Displaying a List of Users, page 15-8](#)
- [Managing Users, page 15-7](#)
- [Guidelines for Managing Users, page 15-8](#)

## Displaying Current User Sessions

You can view a list of the users currently logged into the system and end their sessions, if required. You can see only the users in your available domains.



#### Note

Your user role determines whether you can use this option.

#### Procedure

- Step 1** Select **Admin > Role-Based Access Control > Active Users**.

The Active User Sessions screen displays the following information for each active user who is logged in:

**Table 15-3**      *Active User Session Information*

| Column        | Description                                                 |
|---------------|-------------------------------------------------------------|
| Name          | The name used to log into the ACE appliance Device Manager. |
| Type of Login | Method used to log in, for example WEB or CLI               |
| Login From IP | IP address of host                                          |
| Time Of Login | Time user logged in                                         |

- Step 2** To end an active web session, click **Terminate** (see [Ending Active User Sessions, page 15-12](#) for details). CLI user sessions cannot be ended.

#### Related Topics

- [Deleting Active Users, page 15-12](#)
- [Ending Active User Sessions, page 15-12](#)
- [Displaying a List of Users, page 15-8](#)
- [Managing Users, page 15-7](#)
- [Guidelines for Managing Users, page 15-8](#)

## Deleting Active Users

You can delete users using this procedure. You can also delete users using the **Admin > Role-Based Access Control > Users** menu.

**Note**

Your user role determines whether you can use this option.

**Procedure**

**Step 1** Select **Admin > Role-Based Access Control > Active Users**.

**Step 2** Select the table rows containing the user accounts to be deleted.

**Step 3** Click **Delete**.

The selected users are removed from the ACE Appliance Device Manager.

**Related Topics**

- [Displaying Current User Sessions, page 15-11](#)
- [Ending Active User Sessions, page 15-12](#)
- [Managing Users, page 15-7](#)

## Ending Active User Sessions

When a user session is ended, the user is logged out of the interface from which the user session was initiated. If the user was making changes to a configuration, the configuration lock is released and any uncommitted configuration change is discarded.

If a user session is ended while an operation is in progress, the current operation is not stopped, but any subsequent operation is denied.

**Note**

Your user role determines whether you can use this option.

**Procedure**

**Step 1** Select **Admin > Role-Based Access Control > Active Users**.

**Step 2** Select the table rows containing the user sessions to be ended.

**Step 3** Click **Terminate**.

The selected users are forced out of the system.

**Related Topics**

- [Displaying Current User Sessions, page 15-11](#)
- [Deleting Active Users, page 15-12](#)
- [Managing Users, page 15-7](#)
- [Controlling Access to the Cisco ACE Appliance, page 15-3](#)

## Changing User Passwords

**Note**

Your user role determines whether you can use this option.

**Procedure**

- Step 1** Select **Admin > Role-Based Access Control > Users**. The table of users is displayed.
- Step 2** Select the user account you want to modify.
- Step 3** Click **Edit**.
- Step 4** Change the password attribute in the attributes table (see [Table 15-2](#)).
- Step 5** Click **Deploy Now** to deploy this configuration and to return to the Users table.

**Related Topics**

- [Managing Users, page 15-7](#)
- [Changing the Admin Password, page 15-13](#)

## Changing the Admin Password

Each ACE appliance has an admin user account built into the device. The root user ID is **admin**, and the password is set when the system is installed. For information about changing the Admin password, see [Changing Your Account Password, page 1-6](#).

# Managing User Roles

Use the Roles feature to add, modify, and delete user-defined roles. Predefined roles display with grey italic text and background and cannot be deleted or modified.

A user's role determines the tasks the user can access. Each role is associated with permissions or rules that define what feature access this role contains.

The following sections describe how to manage user roles:

- [Guidelines for Managing User Roles, page 15-14](#)
- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)
- [RBAC User Role Requirements Related to Virtual Servers, page 15-27](#)
- [Displaying User Roles, page 15-28](#)
- [Creating User Roles, page 15-28](#)
- [Modifying User Roles, page 15-30](#)
- [Deleting User Roles, page 15-30](#)

## Guidelines for Managing User Roles

Use these guidelines to manage roles:

- Administrators can view and modify all roles.
- Other users can only view the roles assigned to them.
- You cannot change the default roles.
- Role permissions are different based on whether they were created in an Admin context versus a non-admin or user context. If you want to allow users to switch between contexts, ensure they have a predefined role. If you want to restrict a user to only their home context, assign them a customized user role.
- Certain role features are only available to default roles, for example, an Admin role in the Admin context would have **changeto** and **system** permissions to perform tasks like license management, resource class management, HA setup, and so on. User-created roles cannot use these features.

### Understanding Predefined Roles

The predefined roles and their default privileges are defined in [Table 15-4](#). This table includes rule changes for Admin and user contexts (non-admin contexts). For detailed information on role-based access control, see the *Virtualization Guide, Cisco ACE Application Control Engine*. For details on how the predefined roles are mapped to ACE Appliance Device Manager tasks/features, see [Table 15-5](#).

You must have one of the predefined roles in the Admin context in order to use the **changeto** command (which allows users to visit other contexts). Non-admin/user contexts do not have access to the **changeto** command; they can only visit their home context. Context administrators, who have access to multiple contexts, must explicitly log in to other contexts to which they have access.

Table 15-4 Predefined Role Rules for Admin and User Contexts

| Predefined Role/Context     | Description                                                                                                                                                  | Operations                                                                                                       | Features                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Admin Role</b>           |                                                                                                                                                              |                                                                                                                  |                                                                                                                                                                                                                                                                                                                             |
| Admin Context               | If created in the Admin context, user has complete access to and control over all contexts, domains, roles, users, resources, and objects in the entire ACE. | <ul style="list-style-type: none"> <li>• Debug</li> <li>• Create</li> <li>• Modify</li> <li>• Monitor</li> </ul> | <ul style="list-style-type: none"> <li>• All (context service configuration)</li> <li>• User Access (roles, domains, and users)</li> <li>• System (context administration)</li> <li>• <b>changeto</b> command (access to all contexts)</li> <li>• <b>exec</b> command (enables all default custom role commands)</li> </ul> |
| User Context                | If created in a user context, user has complete access to and control over all objects in that context.                                                      | Create                                                                                                           | <ul style="list-style-type: none"> <li>• All</li> <li>• User Access</li> </ul>                                                                                                                                                                                                                                              |
| <b>Network-Admin Role</b>   |                                                                                                                                                              |                                                                                                                  |                                                                                                                                                                                                                                                                                                                             |
| Admin Context               | Admin for L3 (IP and Routes) and L4 VIPs                                                                                                                     | Create                                                                                                           | <ul style="list-style-type: none"> <li>• Interfaces</li> <li>• Routing</li> <li>• Connection Parameters</li> <li>• Network Address Translation (NAT)</li> <li>• VIPs</li> <li>• Copy Configurations<sup>1</sup></li> <li>• <b>changeto</b> command</li> <li>• <b>exec</b> command</li> </ul>                                |
| User Context                | Access to L3 (IP and Routes) and L4 VIPs                                                                                                                     | Create                                                                                                           | <ul style="list-style-type: none"> <li>• Interfaces</li> <li>• Routing</li> <li>• Connection Parameters</li> <li>• Network Address Translation (NAT)</li> <li>• VIPs</li> <li>• Copy Configurations<sup>1</sup></li> </ul>                                                                                                  |
| <b>Network-Monitor Role</b> |                                                                                                                                                              |                                                                                                                  |                                                                                                                                                                                                                                                                                                                             |
| Admin Context               | Monitoring for all features                                                                                                                                  | Monitor                                                                                                          | <ul style="list-style-type: none"> <li>• All <b>show</b> commands</li> <li>• <b>changeto</b> command</li> <li>• <b>exec</b> command</li> </ul>                                                                                                                                                                              |
| User Context                | Monitoring for all features                                                                                                                                  | Monitor                                                                                                          | <ul style="list-style-type: none"> <li>• All <b>show</b> commands</li> </ul>                                                                                                                                                                                                                                                |

Table 15-4 Predefined Role Rules for Admin and User Contexts

| Predefined Role/Context       | Description                                  | Operations | Features                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security-Admin Role           |                                              |            |                                                                                                                                                                                                                                                                                                                                     |
| Admin Context                 | Security features                            | Create     | <ul style="list-style-type: none"><li>• Access Control Lists (ACLs)</li><li>• Application Inspection</li><li>• Connection parameters</li><li>• Authentication, authorization and accounting (AAA)</li><li>• NAT</li><li>• Copy Configurations<sup>1</sup></li><li>• <b>changeto</b> command</li><li>• <b>exec</b> command</li></ul> |
|                               |                                              | Modify     | Interface                                                                                                                                                                                                                                                                                                                           |
| User Context                  | Security features                            | Create     | <ul style="list-style-type: none"><li>• Access Control Lists (ACLs)</li><li>• Application Inspection</li><li>• Connection parameters</li><li>• Authentication, authorization and accounting (AAA)</li><li>• NAT</li><li>• Copy Configurations<sup>1</sup></li></ul>                                                                 |
|                               |                                              | Modify     | Interface                                                                                                                                                                                                                                                                                                                           |
| Server-Appln-Maintenance Role |                                              |            |                                                                                                                                                                                                                                                                                                                                     |
| Admin Context                 | Server maintenance and L7 policy application | Create     | <ul style="list-style-type: none"><li>• Real Servers</li><li>• Server Farms</li><li>• Load balancing</li><li>• Copy Configurations<sup>1</sup></li><li>• Real Server Inservice</li><li>• <b>changeto</b> command</li><li>• <b>exec</b> command</li></ul>                                                                            |
| User Context                  | Server maintenance and L7 policy application | Create     | <ul style="list-style-type: none"><li>• Real Servers</li><li>• Server Farms</li><li>• Load balancing</li><li>• Copy Configurations<sup>1</sup></li><li>• Real Server Inservice</li></ul>                                                                                                                                            |



Table 15-4 Predefined Role Rules for Admin and User Contexts

| Predefined Role/Context | Description                                   | Operations | Features                                                                                                                                                                                                                                                                                           |
|-------------------------|-----------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server-Maintenance Role |                                               |            |                                                                                                                                                                                                                                                                                                    |
| Admin Context           | Server maintenance, monitoring, and debugging | Debug      | <ul style="list-style-type: none"><li>• Server Farms</li><li>• VIPs</li><li>• Probes</li><li>• Load Balancing</li></ul>                                                                                                                                                                            |
|                         |                                               | Create     | <ul style="list-style-type: none"><li>• <b>changeto</b> command</li><li>• <b>exec</b> command</li></ul>                                                                                                                                                                                            |
|                         |                                               | Modify     | <ul style="list-style-type: none"><li>• Real Servers</li><li>• Real Server Inservice</li></ul>                                                                                                                                                                                                     |
| User Context            | Server maintenance, monitoring, and debugging | Debug      | <ul style="list-style-type: none"><li>• Server Farms</li><li>• VIPs</li><li>• Probes</li><li>• Load Balancing</li></ul>                                                                                                                                                                            |
|                         |                                               | Modify     | <ul style="list-style-type: none"><li>• Real Servers</li><li>• Real Server Inservice</li></ul>                                                                                                                                                                                                     |
| SLB-Admin Role          |                                               |            |                                                                                                                                                                                                                                                                                                    |
| Admin Context           | Load-balancing features                       | Create     | <ul style="list-style-type: none"><li>• Real Servers</li><li>• Server Farms</li><li>• VIP</li><li>• Probes</li><li>• Loadbalance</li><li>• NAT</li><li>• Copy Configurations<sup>1</sup></li><li>• Real Server Inservice</li><li>• <b>changeto</b> command</li><li>• <b>exec</b> command</li></ul> |
|                         |                                               | Modify     | Interface                                                                                                                                                                                                                                                                                          |

Table 15-4 Predefined Role Rules for Admin and User Contexts

| Predefined Role/Context | Description             | Operations | Features                                                                                                                                                                                                                           |
|-------------------------|-------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Context            | Load-balancing features | Create     | <ul style="list-style-type: none"><li>• Real Servers</li><li>• Server Farms</li><li>• VIP</li><li>• Probes</li><li>• Loadbalance</li><li>• NAT</li><li>• Copy Configurations<sup>1</sup></li><li>• Real Server Inservice</li></ul> |
|                         |                         | Modify     | Interface                                                                                                                                                                                                                          |
| SSL-Admin Role          |                         |            |                                                                                                                                                                                                                                    |
| Admin Context           | SSL feature features    | Create     | <ul style="list-style-type: none"><li>• SSL</li><li>• PKI</li><li>• Copy Configurations<sup>1</sup></li><li>• <b>changeto</b> command</li><li>• <b>exec</b> command</li></ul>                                                      |
|                         |                         | Modify     | Interface                                                                                                                                                                                                                          |
| User Context            | SSL feature features    | Create     | <ul style="list-style-type: none"><li>• SSL</li><li>• PKI</li><li>• Copy Configurations<sup>1</sup></li></ul>                                                                                                                      |
|                         |                         | Modify     | Interface                                                                                                                                                                                                                          |

1. For a description of the **copy** command, see the *Command Reference, Cisco ACE Application Control Engine*.

#### Related Topics

- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)
- [Controlling Access to the Cisco ACE Appliance, page 15-3](#)
- [Managing Users, page 15-7](#)
- [Managing User Roles, page 15-14](#)
- [Managing Domains, page 15-31](#)

## Role Mapping in ACE Appliance Device Manager

When you are logged into ACE Appliance Device Manager, you see the tasks that you have been given permission to access. [Table 15-5](#) describes the predefined roles and the menu tasks and features available to those roles. Features and menus that are not applicable for your role will not display.

Since the predefined roles encompass all the role types you may need, we encourage you to use them. If you choose to define your own roles, be aware that rules features are not a one-to-one mapping from CLI feature to ACE Appliance Device Manager menu task.

Defining the proper rules for your user-defined role will require you to create a mapping between the features in [Table 15-4](#) and the ACE Appliance Device Manager menu tasks. For example, in order to manage virtual servers, you must select the following six menu features (Real Servers, Server Farms, VIP, Probes, Load Balancing, NAT, and Interface) in your role.

**Note**

---

There are certain features in the ACE Appliance Device Manager that do not have a corresponding feature mapping on the CLI. One example of this feature is class maps. To modify these features you need to select a predefined role that contains at least one feature with the Modify permission on it.

---

For details on predefined roles and their default privileges, see [Table 15-4](#).

Table 15-5 Role Mapping in ACE Appliance Device Manager

| Menu Task                    | Features Available                                 |
|------------------------------|----------------------------------------------------|
| <b>Admin Predefined Role</b> |                                                    |
| Config > Virtual Contexts >  | System > Primary Attributes                        |
|                              | System > Syslog                                    |
|                              | System > SNMP                                      |
|                              | System > Global Policies                           |
|                              | System > Licenses                                  |
|                              | System > Resource Class                            |
|                              | System > Application Acceleration And Optimization |
|                              | Load Balancing > Virtual Servers                   |
|                              | Load Balancing > Real Servers                      |
|                              | Load Balancing > Server Farms                      |
|                              | Load Balancing > Health Monitoring                 |
|                              | Load Balancing > Stickiness                        |
|                              | Load Balancing > Parameter Maps                    |
|                              | Load Balancing > Secure KAL-AP                     |
|                              | SSL > Certificates                                 |
|                              | SSL > Keys                                         |
|                              | SSL > Parameter Maps                               |
|                              | SSL > Chain Group Parameters                       |
|                              | SSL > CSR Parameters                               |
|                              | SSL > Proxy Service                                |
|                              | SSL > Auth Group Parameters                        |
|                              | SSL > Certificate Revocation Lists (CRL)           |
|                              | Security > ACLs                                    |
|                              | Security > Object Groups                           |

**Table 15-5**      *Role Mapping in ACE Appliance Device Manager (continued)*

| Menu Task                         | Features Available                             |
|-----------------------------------|------------------------------------------------|
|                                   | Network > Port Channel Interfaces              |
|                                   | Network > GigabitEthernet Interfaces           |
|                                   | Network > VLAN Interfaces                      |
|                                   | Network > BVI Interfaces                       |
|                                   | Network > Static Routes                        |
|                                   | Network > Global IP DHCP                       |
|                                   | High Availability (HA) > Setup                 |
|                                   | HA Tracking And Failure Detection > Interfaces |
|                                   | HA Tracking And Failure Detection > Hosts      |
|                                   | Expert > Class Maps                            |
|                                   | Expert > Policy Maps                           |
|                                   | Expert > Action Lists                          |
| Config > Operations               | Real Servers                                   |
|                                   | Virtual Servers                                |
| Monitor > Virtual Contexts        | Load Balancing                                 |
|                                   | CPU                                            |
|                                   | Application Acceleration                       |
|                                   | Interfaces                                     |
|                                   | Real Servers                                   |
|                                   | Statistics Collection                          |
|                                   | Probes                                         |
|                                   | Resource Usage                                 |
| Admin > Role-Based Access Control | Ping                                           |
|                                   | Users                                          |
|                                   | Active Users                                   |
|                                   | Roles                                          |
| Admin > Device Management         | Domains                                        |
|                                   | Statistics                                     |
|                                   | Statistics Collection                          |
| Admin > Tools                     | Lifeline Management                            |
|                                   | File Browser                                   |

**Table 15-5**      *Role Mapping in ACE Appliance Device Manager (continued)*

| Menu Task                            | Features Available              |
|--------------------------------------|---------------------------------|
| <b>Network-Admin Predefined Role</b> |                                 |
| Config > Virtual Contexts >          | System > Primary Attributes     |
|                                      | System > Global Policies        |
|                                      | Load Balancing > Parameter Maps |
|                                      | Network > VLAN Interface        |
|                                      | Network > BVI Interfaces        |
|                                      | Network > Static Routes         |
|                                      | Network > Global IP DHCP        |
|                                      | Expert > Class Maps             |
|                                      | Expert > Policy Maps            |
| Config > Operations                  | Virtual Servers                 |
| Monitor >                            | Application Acceleration        |
|                                      | Interfaces                      |
|                                      | Real Servers                    |
|                                      | Probes                          |
|                                      | Resources                       |
|                                      | Ping                            |
| Admin > Tools                        | File Browser                    |

**Table 15-5**      *Role Mapping in ACE Appliance Device Manager (continued)*

| Menu Task                              | Features Available                             |
|----------------------------------------|------------------------------------------------|
| <b>Network-Monitor Predefined Role</b> |                                                |
| Config > Virtual Contexts >            | System > Primary Attributes                    |
|                                        | System > Syslog                                |
|                                        | System > Global Policies                       |
|                                        | Load Balancing > Virtual Servers               |
|                                        | Load Balancing > Real Servers                  |
|                                        | Load Balancing > Server Farms                  |
|                                        | Load Balancing > Health Monitoring             |
|                                        | Load Balancing > Stickiness                    |
|                                        | Load Balancing > Parameter Maps                |
|                                        | Load Balancing > Secure KAL-AP                 |
|                                        | SSL > Certificates                             |
|                                        | SSL > Keys                                     |
|                                        | SSL > Parameter Map                            |
|                                        | SSL > Chain Group Parameters                   |
|                                        | SSL > CSR Parameters                           |
|                                        | SSL > Proxy Service                            |
|                                        | SSL > Auth Group Parameters                    |
|                                        | SSL > Certificate Revocation Lists (CRL)       |
|                                        | Security > ACLs                                |
|                                        | Security > Object Groups                       |
|                                        | Network > VLAN Interfaces                      |
|                                        | Network > BVI Interfaces                       |
|                                        | Network > Static Routes                        |
|                                        | Network > Global IP DHCP                       |
|                                        | HA Tracking And Failure Detection > Interfaces |
|                                        | HA Tracking And Failure Detection > Hosts      |
|                                        | Expert > Class Maps                            |
|                                        | Expert > Policy Maps                           |
|                                        | Expert > Action Lists                          |
| Config > Operations                    | Real Servers                                   |
|                                        | Virtual Servers                                |

Table 15-5 Role Mapping in ACE Appliance Device Manager (continued)

| Menu Task                                       | Features Available              |
|-------------------------------------------------|---------------------------------|
| Monitor >                                       | Load Balancing                  |
|                                                 | Application Acceleration        |
|                                                 | Interfaces                      |
|                                                 | Real Servers                    |
|                                                 | Probes                          |
|                                                 | Resource Usage                  |
|                                                 | Ping                            |
| <b>Security-Admin Predefined Role</b>           |                                 |
| Config > Virtual Contexts >                     | System > Primary Attributes     |
|                                                 | System > Global Policies        |
|                                                 | Load Balancing > Parameter Maps |
|                                                 | Security > ACLs                 |
|                                                 | Security > Object Groups        |
|                                                 | Network > VLAN Interfaces       |
|                                                 | Network > BVI Interfaces        |
|                                                 | Network > Global IP DHCP        |
|                                                 | Expert > Class Maps             |
|                                                 | Expert > Policy Maps            |
| Monitor > Virtual Contexts                      | Resource Usage                  |
|                                                 | Ping                            |
| Admin > Tools                                   | File Browser                    |
| <b>Server-Appln Maintenance Predefined Role</b> |                                 |
| Config > Virtual Contexts >                     | System > Primary Attributes     |
|                                                 | Load Balancing > Real Servers   |
|                                                 | Load Balancing > Server Farms   |
|                                                 | Load Balancing > Parameter Maps |
|                                                 | Expert > Class Maps             |
|                                                 | Expert > Policy Maps            |
|                                                 | Expert > Action Lists           |
| Config > Operations                             | Real Servers                    |
| Monitor > Virtual Contexts                      | Load Balancing                  |
|                                                 | Real Servers                    |
|                                                 | Resource Usage                  |
|                                                 | Ping                            |
| Admin > Tools                                   | File Browser                    |



**Table 15-5**      *Role Mapping in ACE Appliance Device Manager (continued)*

| Menu Task                                 | Features Available                 |
|-------------------------------------------|------------------------------------|
| <b>Server-Maintenance Predefined Role</b> |                                    |
| Config > Virtual Contexts >               | System > Primary Attributes        |
|                                           | Load Balancing > Real Servers      |
|                                           | Load Balancing > Server Farms      |
|                                           | Load Balancing > Health Monitoring |
|                                           | Load Balancing > Parameter Maps    |
|                                           | Expert > Class Maps                |
|                                           | Expert > Policy Maps               |
| Config > Operations                       | Expert > Action Lists              |
|                                           |                                    |
| Monitor > Virtual Contexts                | Real Servers                       |
|                                           | Virtual Servers                    |
|                                           | Load Balancing                     |
|                                           | Real Servers                       |
|                                           | Probes                             |
|                                           | Resource Usage                     |
|                                           | Ping                               |
| <b>SLB-Admin Predefined Role</b>          |                                    |
| Config > Virtual Contexts >               | System > Primary Attributes        |
|                                           | System > Global Policies           |
|                                           | Load Balancing > Virtual Servers   |
|                                           | Load Balancing > Real Servers      |
|                                           | Load Balancing > Server Farms      |
|                                           | Load Balancing > Health Monitoring |
|                                           | Load Balancing > Parameter Maps    |
|                                           | Network > VLAN Interfaces          |
|                                           | Network > BVI Interfaces           |
|                                           | Network > Global IP DHCP           |
|                                           | Expert > Class Maps                |
|                                           | Expert > Policy Maps               |
| Config > Operations                       | Expert > Action Lists              |
|                                           |                                    |
|                                           | Real Servers                       |
|                                           | Virtual Servers                    |

**Table 15-5**      *Role Mapping in ACE Appliance Device Manager (continued)*

| Menu Task                   | Features Available                       |
|-----------------------------|------------------------------------------|
| Monitor > Virtual Contexts  | Load Balancing                           |
|                             | Real Servers                             |
|                             | Probes                                   |
|                             | Resource Usage                           |
|                             | Ping                                     |
| Admin > Tools               | File Browser                             |
| <b>SSL-Admin</b>            |                                          |
| Config > Virtual Contexts > | System > Primary Attributes              |
|                             | System > Global Policies                 |
|                             | Load Balancing > Parameter Maps          |
|                             | SSL > Certificates                       |
|                             | SSL > Keys                               |
|                             | SSL > Parameter Maps                     |
|                             | SSL > Chain Group Parameters             |
|                             | SSL > CSR Parameters                     |
|                             | SSL > Proxy Service                      |
|                             | SSL > Auth Group Parameters              |
|                             | SSL > Certificate Revocation Lists (CRL) |
|                             | Network > VLAN Interfaces                |
|                             | Network > BVI Interfaces                 |
|                             | Network > Global IP DHCP                 |
|                             | Expert > Class Maps                      |
|                             | Expert > Policy Maps                     |
| Monitor > Virtual Contexts  | Resource Usage                           |
|                             | Ping                                     |
| Admin > Tools               | File Browser                             |

**Related Topics**

- [Predefined Role Rules for Admin and User Contexts](#)
- [Controlling Access to the Cisco ACE Appliance, page 15-3](#)
- [Guidelines for Managing User Roles, page 15-14](#)
- [Managing Users, page 15-7](#)
- [Managing User Roles, page 15-14](#)
- [Managing Domains, page 15-31](#)

## RBAC User Role Requirements Related to Virtual Servers

If you want to create, modify, or delete a virtual server, we recommend that you use the pre-defined Admin role (see [Table 15-4](#)). Only the Admin pre-defined role supports the ability to successfully deploy a functional virtual server from the ACE appliance Device Manager.

If a user prefers to be assigned a custom role, and wants the ability to create, modify, or delete a virtual server, that user requires the proper role permissions to be defined by the administrator to allow them to perform those virtual server activities.



**Note**

A user must be assigned with a default domain (default-domain) to be able to configure a virtual server. A domain is the namespace in which a user operates.



**Note**

For a user with a customized role to perform configuration and operation changes from the ACE Appliance Device Manager, you must configure the role with rules that permit the create operation for the config-copy and exec-commands features.

Included below are a list of RBAC permissions which are required for a user to create, modify, or delete a virtual server:

| Rule | Type   | Permission | Feature     |
|------|--------|------------|-------------|
| 1.   | Permit | Create     | real        |
| 2.   | Permit | Create     | serverfarm  |
| 3.   | Permit | Create     | vip         |
| 4.   | Permit | Create     | probe       |
| 5.   | Permit | Create     | loadbalance |
| 6.   | Permit | Create     | nat         |
| 7.   | Permit | Create     | interface   |
| 8.   | Permit | Create     | connection  |
| 9.   | Permit | Create     | ssl         |
| 10.  | Permit | Create     | pki         |
| 11.  | Permit | Create     | sticky      |
| 12.  | Permit | Create     | inspect     |

Note that certain configured virtual servers may only cover a subset of the features and may not require all the permissions outlined above. In general, the above set of permissions are required for allowing users to configure all elements of a virtual server.

## Displaying User Roles

Use this option to display the existing user roles.



### Note

Your user role determines whether you can use this option.

### Procedure

- 
- Step 1** Select **Admin > Role-Based Access Control > Roles**. A table of the defined roles and their settings appears.
- Step 2** You can use the options in this screen to create a new role, filter roles based on a string, or modify or delete any existing role to which you have access.
- Step 3** To view the users assigned to a role, select **Admin > Role-Based Access Control > Users**.
- 

### Related Topics

- [Understanding Operations Privileges, page 15-6](#)
- [Managing User Roles, page 15-14](#)

## Creating User Roles

You can create new, user-defined roles. When you create a new role, you specify a name and description of the new role,, and then then select the operations privileges for each task. You can also assign this role to one or more users.



### Note

Your user role determines whether you can use this option.

### Procedure

- 
- Step 1** Select **Admin > Role-Based Access Control > Roles**. A table of the defined roles and their settings appears.
- Step 2** Click **Add**. The New Role configuration screen appears.
- Step 3** Enter the following attributes.

**Table 15-6**      *Role Attributes*

| Attribute   | Description                      |
|-------------|----------------------------------|
| Name        | The name of the role.            |
| Description | A brief description of the role. |

- Step 4** Click **Deploy Now** to deploy this configuration. The new role is added to the list of user roles and the Rules table appears below the Roles form in the content area.
- Step 5** Click **Add** to create rules for this role. This role inherits the roles of the user that created it.

**Step 6** To alter rules, select changes to any of the following attributes.



**Note**

For a user with a customized role to perform configuration and operation changes from the ACE Appliance Device Manager, you must configure the role with rules that permit the create operation for the config-copy and exec-commands features.

**Table 15-7** *Rule Attributes*

| Attribute   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule Number | The number assigned to this rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Permission  | Permit or deny the specified operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Operation   | Create, debug, modify <sup>1</sup> , and monitor the specified feature.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Feature     | <p>AAA, Access List, Change To Context, Config Copy, Connection, DHCP, Exec-Commands, Fault Tolerant, Inspect, Interface, Load Balance, NAT, PKI<sup>2</sup>, Probe, Real Inservice, Routing, Real Server, Server Farm, SSL<sup>2, 3</sup>, Sticky, Syslog, and VIP.</p> <p>The Changeto feature allows you to move from the Admin context to another virtual context and maintain the same role with the same privileges in the new context that you had in the Admin context.</p> <p>The Exec-commands feature enables all default custom role commands in the ACE. The default custom role commands are capture, debug, gunzip, mkdir, move, rmkdir, tac-pac, untar, write, and undebg.</p> |

1. Certain features are not available for certain operations. For **modify**, the following features cannot be used: Change To Context, Config-Copy, DHCP, Exec-Commands, NAT, Real Inservice, Routing, and Syslog.
2. The PKI and SSL features are not available with the ACE NPE software version (see the [“Information About the ACE No Payload Encryption Software Version”](#) section on page 1-2).
3. For all SSL-related operations, a user with a custom role should include the following two rules: A rule that includes the SSL feature, and a rule that includes the PKI feature.

**Step 7** Click **Deploy Now** to update the rule for this role.

**Related Topics**

- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)
- [Understanding Operations Privileges, page 15-6](#)
- [Managing User Roles, page 15-14](#)

## Modifying User Roles

You can modify any user-defined roles.

**Note**

Your user role determines whether you can use this option.

**Procedure**

- 
- |               |                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select <b>Admin &gt; Role-Based Access Control &gt; Roles</b> . A table of the defined roles and their settings appears. |
| <b>Step 2</b> | Select the role you want to modify.                                                                                      |
| <b>Step 3</b> | Click <b>Edit</b> .                                                                                                      |
| <b>Step 4</b> | Make the changes.                                                                                                        |
| <b>Step 5</b> | Click <b>Deploy Now</b> to deploy this configuration and to return to the Roles table.                                   |
- 

**Related Topics**

- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)
- [Understanding Operations Privileges, page 15-6](#)
- [Managing User Roles, page 15-14](#)

## Deleting User Roles

You can delete any user-defined roles (as long as they are not being used by a user).

**Note**

Your user role determines whether you can use this option.

**Procedure**

- 
- |               |                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select <b>Admin &gt; Role-Based Access Control &gt; Roles</b> . A table of the defined roles and their settings appears.                                      |
| <b>Step 2</b> | Select the role to be deleted.                                                                                                                                |
| <b>Step 3</b> | Click <b>Delete</b> . A prompt asks you to confirm this action. Click <b>OK</b> to delete the role or Cancel to exit the procedure without deleting the role. |
- If you click **OK**, the window refreshes with the Roles table and the deleted user role no longer appears. Users that have the deleted role no longer have that access.
- 

**Related Topic**

[Managing User Roles, page 15-14](#)

## Adding, Editing, or Deleting Rules

You can change or delete rules to redefine what feature access a specific role contains.



**Note**

Your user role determines whether you can use this option.

### Procedure

- 
- Step 1** Select **Admin > Role-Based Access Control > Roles**. A table of the defined roles and their settings appears.
- Step 2** Select the role to be changed. You can only change rules if only one role is selected in the pane.
- Step 3** Perform any of the following tasks:
- Click **Add** to create a new rule. Enter the rule information (see [Table 15-7 on page 15-29](#)), and then click **Deploy Now**.
  - Select a rule and click **Edit** to change an existing rule. Click **Deploy Now** to save this rule.
  - Select the rules to remove from this role and click **Delete**. Click **OK** to confirm its deletion.
- 

### Related Topic

- [Managing User Roles, page 15-14](#)
- [Role Mapping in ACE Appliance Device Manager, page 15-19](#)
- [Guidelines for Managing User Roles, page 15-14](#)

## Managing Domains

Network domains provide a means for organizing the devices and their components (physical and logical) in your network and permitting access according to the way your site is organized.

The following sections describe how to manage domains:

- [Guidelines for Managing Domains, page 15-31](#)
- [Displaying Network Domains, page 15-32](#)
- [Creating Domains, page 15-33](#)
- [Modifying Domains, page 15-34](#)
- [Deleting Domains, page 15-34](#)

## Guidelines for Managing Domains

- Devices and their components must already be configured in ACE Appliance Device Manager in order for them to be added to a domain.
- Domains are *logical* concepts. You do *not* delete a member of a domain when you delete the domain.

- Predefined domains cannot be modified or deleted.
- Normally, a user is associated with the default domain, which allows the user to see all configurations within the context. When a user is configured with a customized domain, then the user can see only what is in the domain.

**Note**

To add objects to a customized domain, use the CLI and then use the synchronize feature in ACE Appliance Device Manager to add this object into its customized domain on ACE Appliance Device Manager. Adding objects to customized domains directly in ACE Appliance Device Manager results in the object being added to the default domain.

**Related Topics**

- [Displaying Network Domains, page 15-32](#)
- [Creating Domains, page 15-33](#)
- [Modifying Domains, page 15-34](#)
- [Deleting Domains, page 15-34](#)

## Displaying Network Domains

**Note**

Your user role determines whether you can use this option.

**Procedure**

- Step 1** Select **Admin > Role-Based Access Control > Domains**. The Domains table appears.
- Step 2** Expand the table until you can see all the network domains.
- Step 3** Select a domain from the Domains table to view the settings for that domain.
- Step 4** You can also perform these tasks from this pane:
  - [Creating Domains, page 15-33](#)
  - [Modifying Domains, page 15-34](#)
  - [Adding or Deleting Domain Objects from a Domain, page 15-35](#)
  - [Deleting Domains, page 15-34](#)

**Related Topic**

- [Managing Domains, page 15-31](#)
- [Guidelines for Managing Domains, page 15-31](#)



## Creating Domains

Use this option to create a new domain.



### Note

Your user role determines whether you can use this option.

### Procedure

- Step 1** Select **Admin > Role-Based Access Control > Domains**. The Domains table appears.
- Step 2** Click **Add**.
- Step 3** Enter the name of the new domain, and then click **Deploy Now**.
- Step 4** Click **Add** in the Domain Object table that displays below the Domain form.
- Step 5** Enter the attributes displayed in [Table 15-8](#).

**Table 15-8**      *Domain Attributes*

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Type | <p>The collection of objects which comprise this domain. The following options may be available depending on your virtual context:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Access List Ethertype</li> <li>• Access List Extended</li> <li>• Class Map</li> <li>• Interface VLAN</li> <li>• Interface BVI</li> <li>• Parameter Map</li> <li>• Policy Map</li> <li>• Probe</li> <li>• Real Server</li> <li>• Script</li> <li>• Server Farm</li> <li>• Sticky</li> </ul> |
| Object Name | This field appears when any specific object type is selected. Name of an existing object defined.                                                                                                                                                                                                                                                                                                                                                                                         |

- Step 6** Click **Deploy Now** to deploy this configuration.

### Related Topic

- [Managing Domains, page 15-31](#)
- [Guidelines for Managing Domains, page 15-31](#)

## Modifying Domains

Use this option to change the settings in a domain.

**Note**

Your user role determines whether you can use this option.

**Procedure**

- 
- Step 1** Select **Admin > Role-Based Access Control > Domains**.
  - Step 2** Select the domain you want to change.
  - Step 3** Click **Edit**.
  - Step 4** Make the changes.
  - Step 5** Click **Deploy Now** to deploy this configuration.
- 

**Related Topics**

- [Managing Domains, page 15-31](#)
- [Guidelines for Managing Domains, page 15-31](#)

## Deleting Domains

Use this option to delete network domains from the system, as well as all the devices and domain objects they contain. You can only delete domains that are not associated with a user.

**Note**

Your user role determines whether you can use this option.

**Procedure**

- 
- Step 1** Select **Admin > Role-Based Access Control > Domains**.  
The Domains table contains a list of the existing domains.
  - Step 2** Select the domain you want to delete.
  - Step 3** Click **Delete**.  
A prompt asks you to confirm this action.
  - Step 4** Click **OK**.  
The domain is deleted from the ACE appliance.
- 

**Related Topics**

- [Managing Domains, page 15-31](#)
- [Guidelines for Managing Domains, page 15-31](#)

## Adding or Deleting Domain Objects from a Domain

Use this option to add or delete a network domain from the system, as well as all the devices and domain objects it contains. You can delete domains that are not associated with a user.



### Note

Your user role determines whether you can use this option.

### Procedure

- 
- Step 1** Select **Admin > Role-Based Access Control > Domains**.  
The Domains table contains a list of the existing domains.
- Step 2** From the Domain table, select a domain in which you want to perform the action.
- Step 3** You can then:
- Add a domain object by clicking **Add** in the Domain Object table and entering the object type and object name (if necessary). Then click **Deploy Now**.
  - Select a row or rows in the Domain Object table that you want to delete and click **Delete**.  
A prompt asks you to confirm this action. Click **OK**. The domain object is deleted from the ACE appliance.
- 

### Related Topics

- [Managing Domains, page 15-31](#)
- [Guidelines for Managing Domains, page 15-31](#)

## Monitoring ACE Appliance Statistics

You can view and set ACE appliance platform statistics data using the following menus:

- Statistics—Displays ACE appliance statistics and allows you to view them graphically. See [Viewing ACE Appliance Server Statistics, page 15-35](#).
- Statistics Collection—Allows you to enable or disable ACE appliance statistic collection. See [Configuring ACE Appliance Server Statistics Collection, page 15-36](#).

## Viewing ACE Appliance Server Statistics

Use this procedure to display ACE appliance statistics (for example, CPU, disk, and memory usage) and view them graphically.

Statistics collection is enabled by default and are collected and saved to database every 5 minutes after the device SNMP credential configuration passes validation and is saved. For a newly created virtual context, the only piece of information that you need to provide in order to start statistical collection is the SNMP community information in the Config > SNMP screen.

To enable or disable ACE appliance statistic collection, see [Configuring ACE Appliance Server Statistics Collection, page 15-36](#).

### Procedure

Select **Admin > Device Management > Statistics**. The ACE appliance statistics shown in [Table 15-9](#) are displayed.

**Table 15-9** *ACE Appliance Server Statistics*

| Name        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Owner       | Process where statistics are collected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Statistic   | Includes the following statistics: <ul style="list-style-type: none"> <li>• CPU Usage—Overall ACE appliance CPU busy percentage in the last 5-minute period.</li> <li>• Disk Usage—Amount of disk space being used by the ACE appliance.</li> <li>• Memory Usage—Amount of memory being used by the ACE appliance.</li> <li>• Process Uptime—Amount of time since this system was last initialized, or the amount of time since the network management portion of the system was last reinitialized.</li> </ul> |
| Value       | Value of the statistic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description | Information the statistic gathered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### Related Topics

- [Monitoring ACE Appliance Statistics, page 15-35](#)
- [Configuring ACE Appliance Server Statistics Collection, page 15-36](#)

## Configuring ACE Appliance Server Statistics Collection

Use this procedure to enable ACE appliance statistics polling from the Monitor menu. The statistics collected include the following:

- CPU Usage—Overall ACE appliance CPU busy percentage in the last 5-minute period.
- Disk Usage—Amount of disk space being used by the ACE appliance.
- Memory Usage—Amount of memory being used by the ACE appliance.
- Process Uptime—Amount of time since this system was last initialized, or the amount of time since the network management portion of the system was last reinitialized.

If you want to set up collection for interface, CPU, load balancing and other statistics per virtual context, see [Setting Up Virtual Contexts Statistics Collection, page 14-33](#).

### Procedure

- Step 1** Select **Admin > Device Management > Statistics Collection**. The Statistics Collection screen appears.
- Step 2** In the Polling Stats field, select **Enable** to start background polling or **Disable** to stop background polling.

- Step 3** In the Background Polling Interval field, select the polling interval appropriate for your networking environment. The interval range is from one minute to six hours.
- Step 4** Click **OK** to save your entries.



**Note** These settings are not saved if you reboot your appliance. The system defaults will be restored.

---

#### Related Topics

- [Monitoring ACE Appliance Statistics, page 15-35](#)
- [Viewing ACE Appliance Server Statistics, page 15-35](#)

## Using Admin Tools

Use these Admin Tools to perform troubleshooting and diagnostics tasks:

- [Generating a Diagnostic Package, page 16-1](#)—Use the troubleshooting and diagnostics tools provided by the Lifeline feature to report a critical problem to the Cisco support line and generate a diagnostic package.
- [Manipulating ACE Appliance Files, page 16-6](#)—Use the File Browser to download or upload files from the ACE appliance for viewing or tracking.

For details about these management tools, see [Using ACE Appliance Device Manager Troubleshooting Tools, page 16-1](#).





# CHAPTER 16

## Using ACE Appliance Device Manager Troubleshooting Tools

---

Use the following diagnostic tools to help troubleshoot ACE Appliance Device Manager problems:

- [Generating a Diagnostic Package, page 16-1](#)
- [Manipulating ACE Appliance Files, page 16-6](#)
- [Checking the ACE Appliance DM GUI Status, page 16-10](#)



### Note

When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (\_), hyphen (-), dot (.), and asterisk (\*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

---

## Generating a Diagnostic Package

Diagnosing network or system-related problems that happen in real time can consume a considerable amount of time and lead to frustration even for a system expert. When a critical problem occurs within the ACE Appliance Device Manager system, you can use the troubleshooting and diagnostics tools provided by the Lifeline feature to report ACE Appliance Device Manager data to the Cisco support line and generate a diagnostic package. Support engineers and developers can subsequently reconstruct your system and debug the problem using the information captured in the Lifeline package.



### Note

To troubleshoot problems related to the ACE appliance, use the **debug** and **show** commands supported in the command line interface (CLI). For a list of the ACE appliance **show** commands, see the *Command Reference, Cisco ACE Application Control Engine*. For more detailed descriptions of hardware and software show commands, see the *Administration Guide, Cisco ACE Application Control Engine*.

---

Lifeline takes a snapshot of the running system configuration, status, buffers, logs, thread dumps, messages, and so on. It gathers a period of historical network and system events that have been recorded directly preceding the event. If required, Lifeline can back up and package the ACE Appliance Device Manager database or a file subdirectory or trace and package a period of traffic flow packets for a specified virtual context.

**Tip**

Do not attempt to use Lifeline without first discussing it with Cisco support.

The following sections describe how to use the Lifeline feature:

- [Guidelines for Using Lifeline, page 16-2](#)
- [Creating a Lifeline Package from the ACE Appliance DM GUI, page 16-3](#)
- [Downloading a Lifeline Package, page 16-3](#)
- [Deleting a Lifeline Package, page 16-4](#)
- [Creating a Lifeline Package from the ACE Appliance CLI, page 16-5](#)

## Guidelines for Using Lifeline

Depending upon the ACE Appliance Device Manager problem you are troubleshooting, Lifelines can be created when unwanted events occur. Under such circumstances, available resources could be extremely low (CPU and memory could be nearly drained). You should be aware of the following:

- Create a Lifeline package after you encounter a problem that might require customer support assistance. The package is meant to be viewed by customer support.
- Lifeline collects debug data from diagnostic generators based on priority – most important to least important. When the total data size reaches 200MB, the collector stops collecting, and data from generators with lower priorities can be lost. For details on content, size, time, state, and any dropped data, see the Readme file included in each Lifeline package.
- Lifeline collects the last 25 MB of data from the file and truncates the beginning content.
- Lifelines are automatically packaged by the system in zip files. The naming convention for a lifeline package is “lifeline-yyMMdd-hhmmss.zip”. For example, lifeline-060622-152140.zip is a Lifeline package created at 3:21:40 PM, June 22, 2006.
- Only one Lifeline package is created at a time. The system will reject a second request made before the first Lifeline has been packaged.
- Lifeline times out in 60 minutes.
- A maximum of 5 Lifeline packages are stored at a time. Files are stored on the RAM disk. You can safely delete these packages after downloading them to store in another location. If you do not delete them, the Lifeline manager performs the cleanup, automatically removing the oldest package first.
- The disk monitor notes when your disk space reaches 80%. Ensure you delete or download your packages so that additional packages can be created.



## Creating a Lifeline Package from the ACE Appliance DM GUI

### Assumptions

- The ACE appliance is running.
- You have reviewed the guidelines for managing lifelines (see [Guidelines for Using Lifeline, page 16-2](#)).
- You have opened a case with Cisco technical support.

### Procedure



**Note**

Your user role determines whether you can use this option.

- Step 1** Select **Admin > Tools > Lifeline Management**.
- Step 2** Enter a description for the package (required). This can include information about why the package is being created, who requested the package, and so forth.
- Step 3** To create a package, click **Save**. A zip file is created in the following format: lifeline-yyMMdd-hhmmss.zip, and displays in the Lifelines pane. The package size, name, and generation date display in the Edit Lifeline window.



**Note**

Do not perform any ACE appliance maintenance until the package is created.

After the package is created, you can:

- Click **Download** to save the package to a directory on your computer—See [Downloading a Lifeline Package, page 16-3](#).
- Click **Add** to return to the add mode from the Edit mode.
- Click **Delete** to delete the package—See [Deleting a Lifeline Package, page 16-4](#).

### Related Topics

- [Generating a Diagnostic Package, page 16-1](#)
- [Downloading a Lifeline Package, page 16-3](#)
- [Deleting a Lifeline Package, page 16-4](#)

## Downloading a Lifeline Package

Use this procedure to download a package for saving to your local drive.

### Assumption

You have created a package (see [Creating a Lifeline Package from the ACE Appliance DM GUI, page 16-3](#)).

**Procedure****Note**


---

Your user role determines whether you can use this option.

---

**Step 1** Select **Admin > Tools > Lifeline Management**.

**Step 2** Select the package from the list.

**Step 3** Click **Download**.

The File Download window displays.

**Step 4** Click **Save**.

The package is sent to your Web browser, where you can save the package.

---

**Related Topics**

- [Generating a Diagnostic Package, page 16-1](#)
- [Creating a Lifeline Package from the ACE Appliance DM GUI, page 16-3](#)
- [Deleting a Lifeline Package, page 16-4](#)

## Deleting a Lifeline Package

Use this procedure to delete a package. You should delete packages you no longer need to free disk space for additional files.

**Procedure****Note**


---

Your user role determines whether you can use this option.

---

**Step 1** Select **Admin > Tools > Lifeline Management**.

**Step 2** Select the package from the list, and then click **Delete**.

A message requests you confirm the deletion.

**Step 3** Click **OK** to delete the package.

---

**Related Topics**

- [Generating a Diagnostic Package, page 16-1](#)
- [Creating a Lifeline Package from the ACE Appliance DM GUI, page 16-3](#)
- [Downloading a Lifeline Package, page 16-3](#)

## Creating a Lifeline Package from the ACE Appliance CLI

If you encounter issues with the ACE appliance Device Manager GUI (for example, when the Device Manager GUI is inoperative), use the **dm lifeline** CLI command from Exec mode to create and upload a lifeline to a remote TFTP server. The **dm lifeline** CLI command is useful when a lifeline cannot be generated from the ACE appliance Device Manager GUI.

**Note**

See the [“Checking the ACE Appliance DM GUI Status” procedure on page 16-10](#) for information on using the `dm status` CLI command to verify the health of the ACE appliance Device Manager.

**Assumptions**

- The ACE appliance is running.
- You have opened a case with Cisco technical support.
- You are the global administrator; the **dm lifeline** CLI command is only available to the global administrator.
- The TFTP server is reachable and is able to receive files from the ACE appliance.

**Procedure****Note**

Your user role determines whether you can use this option.

**Step 1** Log into the ACE by entering the login username and password at the following prompt:

```
switch login: admin
Password: xxxxxx
```

**Step 2** Enter the **dm lifeline tftp** CLI command using the following syntax:

**dm lifeline tftp** <host> [*port*]

The keywords, arguments, and options are as follows:

- **host**—Specifies the TFTP network server.
- *port*—(Optional) Port number.

A file is created and uploaded to the specified TFTP server in the following format: `anm-lifeline.tar.gz`. The file is copied to the root directory of the TFTP server.

# Manipulating ACE Appliance Files

File Browser provides access to the ACE appliance to download or upload multiple files for viewing or tracking. This tool can be also be used to rename files or view logs or other files that help you manage your network or locate problems on the ACE appliance. You can also use this feature to copy an existing context package capture buffer to a remote server.

- [About File Browser, page 16-6](#)
- [Downloading Files, page 16-7](#)
- [Uploading Files, page 16-7](#)
- [Renaming Files, page 16-8](#)
- [Deleting Files, page 16-9](#)
- [Viewing Files, page 16-9](#)

**Note**

To manage license files, use the Licenses screen in the Config tab (**Config > Virtual Contexts > System > Licenses**). To manage Lifeline packages, use the Lifeline screen in the Admin tab (**Admin > Tools > Lifeline Management**).

## About File Browser

When using File Browser, keep the following in mind:

- All predefined admin roles, the Server-Appln-Maintenance role, and any customized user roles that include Copy Configuration and permissions greater than monitor have access to the File Browser.
- The object selector contains names of virtual directories that map to real directories on the ACE appliance. Although these names are consistent with the CLI **dir** command, the actual directory names on disk are different.
- Select the folder to display its contents. Select the directory name to reload the specific directory.
- There is a size limit imposed on files that are viewed. in File Browser. ACE Appliance Device Manager displays only the first 100 KB and truncates the remaining file.

**Related Topics**

- [Downloading Files, page 16-7](#)
- [Uploading Files, page 16-7](#)
- [Renaming Files, page 16-8](#)
- [Deleting Files, page 16-9](#)
- [Viewing Files, page 16-9](#)

## Downloading Files

Use this feature to download multiple files from the ACE appliance for viewing or tracking. For example, you may want to download logs and view them.

**Note**

Your user role determines whether you can use this option.

### Procedure

- Step 1** Select **Admin > Tools > File Browser**.
- Step 2** Use the drop-down list to select a directory and locate the files you want to download. Traverse the folder structure until you locate the files.
- Step 3** Select the file names in the content pane, and then click **Download**.  
The File Download window displays.
- Step 4** Save the file to your computer.

### Related Topics

- [Uploading Files, page 16-7](#)
- [Viewing Files, page 16-9](#)
- [Renaming Files, page 16-8](#)
- [Deleting Files, page 16-9](#)
- [About File Browser, page 16-6](#)

## Uploading Files

Use this feature to upload files from your PC to the ACE appliance for viewing or tracking.

**Note**

Your user role determines whether you can use this option.

### Procedure

- Step 1** Select **Admin > Tools > File Browser**.
- Step 2** Use the drop-down list to select a directory. Traverse the folder structure until you locate the folder in where you want to upload the file.
- Step 3** Click **Upload**.
- Step 4** Click **Browse** to select the file names to upload from your PC, and then click **OK**.  
The files are uploaded to your ACE appliance.

**Related Topics**

- [Downloading Files, page 16-7](#)
- [Viewing Files, page 16-9](#)
- [Renaming Files, page 16-8](#)
- [Deleting Files, page 16-9](#)
- [About File Browser, page 16-6](#)

## Renaming Files

Use this feature to rename files on the ACE appliance.

**Note**

---

Your user role determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Admin > Tools > File Browser**.
- Step 2** Use the drop-down list to select a directory and locate the files you want to rename. Traverse the folder structure until you locate the file.
- Step 3** Select a file you want to rename. You can only rename one file at a time.
- Step 4** Click **Rename**.
- Step 5** Enter the new name of the file and click **OK**.
- The file is renamed on your ACE appliance.
- 

**Related Topics**

- [Uploading Files, page 16-7](#)
- [Downloading Files, page 16-7](#)
- [Viewing Files, page 16-9](#)
- [Deleting Files, page 16-9](#)
- [About File Browser, page 16-6](#)

## Deleting Files

Use this feature to delete files from the ACE appliance.



**Note**

Your user role determines whether you can use this option.

### Procedure

- 
- Step 1** Select **Admin > Tools > File Browser**.
- Step 2** Use the drop-down list to select a directory and locate the files you want to delete. Traverse the folder structure until you locate the files.
- Step 3** Select the file names in the content pane, and then click **Delete**.  
A window appears requesting confirmation for the deletion.
- Step 4** Click **OK** to delete the named files.  
The files are removed from your ACE appliance.
- 

### Related Topics

- [Uploading Files, page 16-7](#)
- [Downloading Files, page 16-7](#)
- [Viewing Files, page 16-9](#)
- [Renaming Files, page 16-8](#)
- [About File Browser, page 16-6](#)

## Viewing Files

Use this feature to view files from the ACE appliance. You may want to view logs or other files that help you manage your network. Files larger than 100K are truncated when viewing.



**Note**

Your user role determines whether you can use this option.

### Procedure

- 
- Step 1** Select **Admin > Tools > File Browser**.
- Step 2** Use the drop-down list to select a directory and locate the files you want to view. Traverse the folder structure until you locate the files.
- Step 3** Select the file names in the content pane, and then click **View**.  
A new window appears below the existing browser.
- Step 4** To remove the viewed files from the screen and return to the file browser content pane, click **UnView**.
-

**Related Topics**

- [Uploading Files, page 16-7](#)
- [Downloading Files, page 16-7](#)
- [Renaming Files, page 16-8](#)
- [Deleting Files, page 16-9](#)
- [About File Browser, page 16-6](#)

## Checking the ACE Appliance DM GUI Status

If you find that the ACE appliance Device Manager GUI appears to be inoperative, enter the **dm status** CLI command in Exec mode to verify the health of the Device Manager. The **dm status** command output indicates the status of the Device Manager: whether it is running or stopped. This status is reflected in the DM and MySQL fields of the status output.

**Note**

You must be the global administrator to access the **dm status** CLI command. This command is only available to the global administrator.

For example, enter:

```
switch/Admin# dm status
DM ROOT:
DM HOME: /opt/CSCOanm
JAVA_HOME: /opt/CSCOanm/jre
MYSQL_HOME: /opt/CSCOanm/mysql
java is /opt/CSCOanm/jre/bin/java

DM : STOPPED (1230)
MySQL : STOPPED (1187)
```

If you see that the status is “STOPPED,” restart the Device Manager using the **dm reload** command. You must be the global administrator to access the **dm reload** command. Restarting the Device Manager does not impact ACE functionality; however, it may take a few minutes for the Device Manager to reinitialize as it reads the ACE CLI configuration.

Reenter the **dm status** CLI command in Exec mode to verify that the status of the Device Manager is “RUNNING.”

For example, enter:

```
switch/Admin# dm status
DM ROOT:
DM HOME: /opt/CSCOanm
JAVA_HOME: /opt/CSCOanm/jre
MYSQL_HOME: /opt/CSCOanm/mysql
java is /opt/CSCOanm/jre/bin/java

DM : RUNNING (1230)
MySQL : RUNNING (1187)
```





## GLOSSARY

---

### A

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACL</b>                     | Access Control List. A mechanism in computer security used to enforce privilege separation. An ACL identifies the privileges and access rights a user or client has to a particular object, such as a server, file system, or application.                                                                                                                                                                                                                                                                                                                             |
| <b>activate</b>                | Places an entity into the resource pool for load balancing content requests or connections and starts the keepalive function. <i>See also</i> <a href="#">suspend</a> .                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>administrative distance</b> | <p>The first criterion a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. Administrative distance is a measure of the trustworthiness of the source of the routing information. Administrative distance has only local significance, and is not advertised in routing updates.</p> <p>The smaller the administrative distance value, the more reliable the protocol. The values range from 0 (zero) for a connected interface and 1 for a static route, to 255 for an unknown protocol.</p> |
| <b>AES</b>                     | Advanced Encryption Standard. One of the possible encryption algorithms available for use in SNMP communications.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>ARP</b>                     | Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

### B

|            |                                                                                                                                                         |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>BVI</b> | Bridge-Group Virtual Interface. Logical Layer 3-only interface associated with a bridge group when integrated routing and bridging (IRB) is configured. |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### C

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CCM</b>                         | Cisco CallManager. A Cisco product that provides the software-based, call-processing component of the Cisco IP Telephony Solutions for the Enterprise, part of Cisco AVVID (Architecture for Voice, Video, and Integrated Data). CallManager acts as a signaling proxy for call events initiated over other common protocols such as <a href="#">SIP</a> , ISDN (Integrated Services Digital Network), or MGCP (Media Gateway Control Protocol). |
| <b>certificate chain</b>           | A certificate chain is a hierarchal list of certificates used in SSL that includes the subject's certificate, the root CA certificate, and any intermediate CA certificates.                                                                                                                                                                                                                                                                     |
| <b>certificate signing request</b> | See <a href="#">CSR</a> .                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>checkpoint</b> | A snapshot in time of a known stable ACE running configuration before you begin to modify it. If you encounter a problem with the modifications to the running configuration, you can roll back the configuration to the previous stable configuration checkpoint.                                                                                                                                          |
| <b>Cisco.com</b>  | Replaces the Cisco Connection Online Web site. Use this site to access customer service and support.                                                                                                                                                                                                                                                                                                        |
| <b>class map</b>  | A mechanism for classifying types of network traffic. The ACE Appliance Device Manager uses class maps to classify the network traffic that is received and transmitted by the ACE appliance. Types of traffic include Layer 3/Layer 4 traffic that can pass through the ACE appliance, network management traffic that can be received by the ACE appliance, and Layer 7 HTTP load-balancing traffic.      |
| <b>CSR</b>        | Certificate Signing Request. A message sent to a certificate authority, such as VeriSign and Thawte to apply for a digital identity certificate for use with SSL. The request includes information that identifies the SSL site, such as location and serial number, and a public key that you choose. The request may also provide any additional proof of identity required by the certificate authority. |
| <b>context</b>    | See <a href="#">virtual context</a> .                                                                                                                                                                                                                                                                                                                                                                       |

---

## D

|                           |                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DES</b>                | Data Encryption Standard. One of the possible encryption algorithms available for use in SNMP communications.                                                                        |
| <b>DFP</b>                | Dynamic Feedback Protocol. A protocol that allows load-balanced servers (both local and remote) to dynamically report changes in their status and their ability to provide services. |
| <b>distinguished name</b> | Used for SSL, a set of attributes that provides the certificate authority with the information it needs to authenticate your site.                                                   |

---

## E

|                   |                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>event</b>      | A message from the ACE Appliance Device Manager that informs you of activities on parts of the system, including each virtual context, the management system, and hardware components. |
| <b>event type</b> | Alarm, Log, Audit, Attack Log                                                                                                                                                          |
| <b>exception</b>  | A group of related faults.                                                                                                                                                             |

---

## F

|                               |                                                                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>fault</b>                  | An abnormal condition that occurs when a system component exceeds a performance threshold or is not functioning properly.                                      |
| <b>File Transfer Protocol</b> | See <a href="#">FTP</a> .                                                                                                                                      |
| <b>FTP</b>                    | File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959. |

---

H

**HSRP** Hot Standby Router Protocol. A networking protocol that provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

---

I

**ICMP** Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

**Internet Control Message Protocol.** *See* [ICMP](#).

**interface**

1. A network connection.
2. A connection between two systems or devices.
3. In telephony, a shared boundary defined by common physical interconnection characteristics, signal characteristics, and meanings of interchanged signals.

---

L

**load balancing** An action that spreads network requests among available servers within a cluster of servers, based on a variety of algorithms.

---

M

**MD5** Message Digest 5 or Message-Digest Algorithm. One of the possible encryption algorithms available for use in SNMP communications.

**MIB** Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

---

N

**NAT** Name Address Translation. A method of connecting multiple computers to the Internet (or any other IP network) using one IP address.

---

O

|                     |                                                                                                                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>object</b>       | A physical entity, service, or resource that can be managed using ACE Appliance Device Manager.                                                                                                                            |
| <b>object group</b> | A logical grouping of similar objects, such as servers, clients, services, or networks. Creating an object group allows you to apply common attributes to a number of objects without specifying each object individually. |

---

P

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PAT</b>  | Port Address Translation. A mechanism that allows many devices on a LAN to share one IP address by allocating a unique port address at Layer 4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>PEM</b>  | Privacy Enhanced Mail. Internet e-mail that provides confidentiality, authentication, and message integrity using various encryption methods. Not widely deployed in the Internet.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>ping</b> | <p>A common method for troubleshooting the accessibility of devices.</p> <p>A ping tests an ICMP echo message and its reply. Because ping is the simplest test for a device, it is the first to be used.</p> <p>Run ping to view the packets transmitted, packets received, percentage of packet loss, and round-trip time in milliseconds.</p>                                                                                                                                                                                                                                                                      |
| <b>PKCS</b> | Public-Key Cryptography Standards. A series of specifications published by RSA Laboratories for data structures and algorithm usage for basic applications of asymmetric cryptography.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>port</b> | <ol style="list-style-type: none"> <li>1. An interface on an internetworking device (such as a router); a physical entity.</li> <li>2. In IP terminology, an upper-layer process that receives information from lower layers. Ports are numbered, and each numbered port is associated with a specific process. For example, SMTP is associated with port 25. A port number is also called a well-known address.</li> <li>3. To rewrite software or microcode so that it will run on a different hardware platform or in a different software environment than that for which it was originally designed.</li> </ol> |

---

R

|                    |                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RAS</b>         | Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper. |
| <b>RBAC</b>        | Role-Based Access Control. A mechanism that allows privileges to be assigned to defined roles. The roles are then assigned to real users, allowing or limiting access to specific features as appropriate for each role.                                                                              |
| <b>real server</b> | A real server is a physical device assigned to a server farm.                                                                                                                                                                                                                                         |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>redundancy</b>                       | In internetworking, the duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.                                                                                                                                                                                                                                                                                                                                                   |
| <b>resource class</b>                   | A defined set of resources and allocations available for use by a device (such as an ACE appliance). Using resource classes prevents a single device from using all available resources.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>role</b>                             | <i>See</i> <a href="#">user role</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>RSA</b>                              | Rivest, Shamir, and Adelman Signatures. A public-key cryptographic system used for authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>RTSP</b>                             | Real Time Streaming Protocol. A client-server multimedia presentation control protocol, designed to address the needs for efficient delivery of streamed multimedia over IP networks.                                                                                                                                                                                                                                                                                                                                                                     |
| <hr/>                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>S</b>                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>SCCP</b>                             | Skinny Client Control Protocol. A proprietary terminal control protocol owned and defined by Cisco as a messaging set between a skinny client and the Cisco CallManager ( <a href="#">CCM</a> ). Examples of skinny clients include the Cisco 7900 series of IP phone such as the Cisco 7960, Cisco 7940 and the 802.11b wireless Cisco 7920, along with Cisco Unity voicemail server. <i>See also</i> <a href="#">Skinny</a> .                                                                                                                           |
| <b>server farm</b>                      | A collection of servers that contain the same content.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Server Load Balancer</b>             | <i>See</i> <a href="#">SLB</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>service</b>                          | A destination location where a piece of content resides physically. Also referred to in general terms for this release as including content rules, owners, virtual servers, real servers, and so on.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Simple Message Transfer Protocol</b> | <i>See</i> <a href="#">SMTP</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>SIP</b>                              | Session Initiation Protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.                                                                                                                                                                                                                                                                             |
| <b>Skinny</b>                           | Skinny is a lightweight protocol which allows for efficient communication with Cisco CallManager. <i>See also</i> <a href="#">SCCP</a> .                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>SLB</b>                              | Server Load Balancer. A device that makes load balancing decisions based on application availability, server capacity, and load distribution algorithms, such as round robin or least connections. Using load balancing and server/application feedback, an SLB device determines a real server for the packet flow and sends this information to the requesting forwarding agent. After the optimal destination is decided on, all other packets in the packet flow are directed to a real server by the forwarding agent, increasing packet throughput. |
| <b>special configuration file</b>       | Managed file resource on an ACE appliance, such as a piece of a configuration file or a keep-alive script.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>SMTP</b>                             | Simple Message Transfer Protocol. Internet protocol that provides e-mail services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                |                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>sticky</b>  | A feature that ensures that the same client gets the same server for multiple connections. It is used when applications require a consistent and constant connection to the same server. If you are connecting to a system that keeps state tables about your connection, sticky allows you to get back to the same real server again and retain the statefulness of the system. |
| <b>suspend</b> | Removes an entity from the resource pool for future load-balancing content requests or connections. Suspending a service or device does not affect existing content flows, but it prevents additional connections from accessing the suspended entity or content. <i>See also</i> <a href="#">activate</a> .                                                                     |

---

## T

|                                   |                                                                                                                                                                                                                   |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TCP</b>                        | Transport Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.                                          |
| <b>threshold</b>                  | A range in which you expect your network to perform. If a threshold is exceeded or goes below the expected bounds, you examine the areas for potential problems. You can create thresholds for a specific device. |
| <b>traceroute</b>                 | A diagnostic tool that helps you understand why ping fails or why applications time out. Using it, you can view each hop (or gateway) on the route to your device and how long each took.                         |
| <b>Transport Control Protocol</b> | <i>See</i> <a href="#">TCP</a> .                                                                                                                                                                                  |

---

## U

|                  |                                                                                                                                                                                                                                                                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URI</b>       | Uniform Resource Identifier. Type of formatted identifier that encapsulates the name of an Internet object, and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces. [RFC 1630] |
| <b>user role</b> | A mechanism for granting access to features and functionality to a user account.                                                                                                                                                                                                                                                  |

---

## V

|                               |                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>virtual context</b>        | A concept that allows users to partition an ACE appliance into multiple virtual devices. Each virtual context contains its own set of policies, interfaces, resources, and administrators, allowing administrators to more efficiently manage system resources and services.                                                                    |
| <b>VLAN</b>                   | Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible. |
| <b>VLAN Trunking Protocol</b> | <i>See</i> <a href="#">VTP</a> .                                                                                                                                                                                                                                                                                                                |
| <b>virtual server</b>         | A virtual server represents groups of real servers and are associated with a real server farm.                                                                                                                                                                                                                                                  |

|                   |                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VTP</b>        | VLAN Trunking Protocol. A Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations. |
| <b>VTP domain</b> | Also called a VLAN management domain, a domain composed of one or more network devices that share the same VTP domain name and that are interconnected with trunks.                                                                                                                                                                                                                     |

---

## W

|                   |                                                                  |
|-------------------|------------------------------------------------------------------|
| <b>Web server</b> | A machine that contains Web pages that are accessible by others. |
|-------------------|------------------------------------------------------------------|







## INDEX

---

### A

#### acceleration

- configuring [5-57](#)
- configuring globally on ACE [13-9](#)
- overview [13-2](#)
- traffic policies [13-2](#)
- typical configuration flow [13-2](#)

#### access control, configuring on VLAN interfaces [10-18](#)

#### account password [1-6](#)

#### accounts

- see also users
- user, managing [15-7](#)

#### ACE

- class map
  - match conditions [12-9](#)
- license
  - details [4-34](#)
- parameter maps [8-1](#)
- policy map
  - configuring [12-34](#)
  - rules and actions [12-36](#)
- traffic policies [12-2](#)
- viewing license details [4-34](#)

#### ACE appliance

- licenses
  - configuration [4-34](#)
  - importing [4-30](#)
  - managing [4-29](#)
  - removing [4-33](#)
  - statistics [4-34](#)
  - updating [4-32](#)
  - viewing [4-29](#)

#### parameter maps [8-1](#)

#### policy maps [12-34](#)

#### traffic policies [12-2](#)

#### ACE Appliance Device Manager

##### button descriptions

- in monitor screens [1-16](#)
- in tables [1-11](#)

##### icon descriptions

- in monitor screens [1-16](#)
- in tables [1-11](#)

##### inoperative GUI, verifying [16-10](#)

##### logging in [1-4](#)

##### overview [1-6](#)

##### password, changing [1-6](#)

##### reloading [16-10](#)

##### table

- buttons [1-16](#)
- conventions [1-12](#)
- customizing [1-14](#)
- icons [1-16](#)

##### terminology [1-22](#)

##### verifying GUI operational status [16-10](#)

#### ACE appliance server

- configuring attributes [15-36](#)
- polling, enabling [15-36](#)
- statistics [15-35](#)

#### ACE license

- details [4-34](#)

#### ACE network topology

- overview [3-9](#)

#### ACE No Payload Encryption (NPE) software version [1-2](#)

#### ACE Payload Encryption (PE) software version [1-2](#)

#### ACL

- configuration overview [4-58](#)
- configuring
  - EtherType attributes [4-67](#)
  - extended ACL attributes [4-61](#)
  - for VLANs [10-18](#)
  - object groups [4-70](#)
- definition [GL-1](#)
- deleting [4-69](#)
- objects
  - ICMP service parameters [4-76](#)
  - IP addresses [4-71](#)
  - protocols [4-73](#)
  - subnet objects [4-72](#)
  - TCP/UDP service parameters [4-73](#)
- resequencing [4-66](#)
- viewing by context [4-68](#)
- ACL object group
  - configuring [4-70](#)
  - network objects
    - IP addresses [4-71](#)
    - subnet objects [4-72](#)
  - service objects
    - ICMP service parameters [4-76](#)
    - protocols [4-73](#)
    - TCP/UDP service parameters [4-73](#)
- action, setting for policy maps [12-36](#)
- action list
  - application acceleration, configuring [13-3](#)
  - configuration overview [12-90](#)
  - header insertion, rewrite, and deletion [12-92](#)
  - HTTP header modify, configuring [12-90](#)
  - optimization configuration options [5-60, 13-4](#)
  - SSL header insert [12-97](#)
  - SSL URL rewrite [12-95](#)
- activate
  - definition [GL-1](#)
  - real servers [6-10](#)
  - virtual servers [5-64](#)
- adding
  - domain objects [15-35](#)
  - domains [15-33](#)
  - new users [15-8](#)
  - resource classes [4-38](#)
  - roles [15-28](#)
  - SSL
    - parameter map cipher info [9-22](#)
- admin
  - changing passwords [15-13](#)
  - logging in for the first time [1-4](#)
  - menu options [15-2](#)
- Admin context, first virtual context [4-2](#)
- administrative distance, definition [GL-1](#)
- Admin user, add to context [4-6](#)
- advanced editing mode [1-14](#)
- AES, definition [GL-1](#)
- alias IP address
  - assigning to a VLAN [1-21](#)
- all-match policy map [12-34](#)
- All Virtual Contexts table [4-84](#)
- ANM
  - homepage [2-1, 2-2](#)
- application acceleration
  - configuring [5-57](#)
  - configuring globally on ACE [13-9](#)
  - monitoring [14-29](#)
  - overview [13-2](#)
  - traffic policies [13-2](#)
  - typical configuration flow [13-2](#)
- application protocol inspection
  - ILS [12-7](#)
  - limitations [12-6](#)
  - NAT and PAT support [12-6](#)
  - SCCP [12-7](#)
  - SIP [12-7](#)
  - standards [12-6](#)
  - supported protocols [12-6](#)
- archive
  - directory structure and filenames [4-50](#)

naming convention of context files [4-50](#)

overview of configuration [4-49](#)

## ARP

definition [GL-1](#)

## attributes

BVI interfaces [10-23](#)

DNS probes [6-48](#)

Echo-TCP probes [6-48](#)

Finger probes [6-49](#)

for sticky group types [7-16](#)

FTP probes [6-50](#)

health monitoring [6-44](#)

high availability [11-9](#)

HTTP content sticky group [7-16](#)

HTTP cookie sticky group [7-17](#)

HTTP header sticky group [7-18](#)

HTTP parameter maps [8-2](#)

HTTP probes [6-50](#)

HTTPS probes [6-52](#)

IMAP probes [6-54](#)

IP netmask sticky group [7-18](#)

Layer 3/Layer 4 management class map match conditions [12-15](#)

Layer 4 payload sticky group [7-19](#)

## parameter map

connection [8-5](#)

DNS [8-24](#), [8-25](#)

generic [8-18](#)

optimization [8-11](#)

RTSP [8-19](#)

SIP [8-20](#)

Skinny [8-22](#)

POP probes [6-55](#)

predictor method [5-46](#), [6-30](#)

## RADIUS

sticky groups [7-20](#)

RADIUS probes [6-56](#)

real servers [6-6](#)

resource classes [4-37](#)

## RTSP

header sticky groups [7-20](#)

probes [6-56](#)

scripted probes [6-57](#)

server farms [5-37](#), [6-19](#)

SIP-TCP probes [6-59](#)

SIP-UDP probes [6-59](#)

SMTP probes [6-60](#)

SNMP [4-19](#)

SNMP probes [6-60](#)

## SSL

certificate bulk import [9-10](#)

certificate export [9-17](#)

certificate import [9-9](#)

key export [9-18](#)

key pair bulk import [9-14](#)

key pair import [9-13](#)

parameter map cipher info [9-22](#)

sticky groups [7-21](#)

## SSL initiation

for virtual servers [5-53](#)

## SSL termination

for virtual servers [5-19](#)

sticky group [7-12](#)

TCP probes [6-61](#)

Telnet probes [6-62](#)

UDP probes [6-63](#)

virtual contexts [4-11](#)

virtual servers [5-8](#)

VLAN interfaces [10-10](#)

VM probes [6-65](#)

audience, intended [iii-xv](#)

auth group certificate, configuring for SSL [9-32](#)

auto-synchronization of contexts [4-80](#)

## B

## backup

archive directory structure and filenames [4-50](#)

- configuring device configuration [4-52](#)
- defaults [4-52](#)
- guidelines and limitations of [4-51](#)
- overview of configuration [4-49](#)
- bandwidth optimization, configuring [5-58](#)
- buddy sticky group [7-6](#)
- bulk import
  - SSL certificate attributes [9-10](#)
  - SSL key pair attributes [9-14](#)
- button descriptions
  - common buttons [1-9](#)
  - in monitor screens [1-16](#)
  - in tables [1-11](#)
- BVI, definition [GL-1](#)
- BVI interfaces
  - attributes [10-23](#)
  - configuring [10-23](#)
  - secondary IP groups for [10-24](#)
  - viewing by context [10-30](#)

---

## C

- caution, when allocating resources [4-38](#)
- certificate
  - exporting for SSL [9-16](#)
  - importing for SSL [9-8](#)
  - overview of SSL [9-6](#)
- certificate chain, definition [GL-1](#)
- certificate signing request (CSR), definition [GL-2](#)
- chain group certificate, configuring for SSL [9-25](#)
- chain group parameters, configuring for SSL [9-25](#)
- changeto command [15-15](#)
- changing
  - account password [1-6](#)
  - admin password [15-13](#)
  - login password [1-6](#)
  - role rules [15-31](#)
  - user passwords [15-13](#)
- checkpoint, configuration

- comparing with running configuration [4-48](#)
- creating [4-46](#)
- deleting [4-47](#)
- displaying [4-49](#)
- rolling back to [4-48](#)
- Cisco
  - security guidelines [iii-xix](#)
  - What's New [iii-xix](#)
- class map
  - ACE device support [12-9](#)
  - configuring [12-8](#)
  - definition [GL-2](#)
  - deleting [12-8, 12-10](#)
  - match conditions
    - for deep packet inspection [12-25](#)
    - for FTP command inspection [12-30](#)
    - for Layer 7 load balancing [12-16](#)
    - for management traffic [12-14](#)
    - for network traffic [12-11](#)
    - generic server load balancing [12-19](#)
    - Layer 7 SIP deep packet inspection [12-31](#)
    - RADIUS server load balancing [12-20](#)
    - RTSP server load balancing [12-21](#)
    - SIP server load balancing [12-23](#)
  - match types [12-11, 12-14, 12-16, 12-25, 12-30](#)
  - overview [5-1, 6-1, 12-2, 12-3](#)
  - setting match conditions [12-10](#)
  - use with real servers [6-3](#)
  - virtual-address match type attributes [12-11](#)
- command inspection class maps, setting match conditions [12-30](#)
- configuration
  - auto-synchronizing [4-80](#)
  - backup of [4-52](#)
  - CLI synchronization status [4-80](#)
  - high-level flow [1-18](#)
  - overview [1-18](#)
  - restore of [4-55](#)
  - synchronizing

- for high availability [11-6](#)
  - virtual context [4-79](#)
- task overview [1-18](#)
- viewing status [4-80](#)
- configuration attributes
  - extended ACL [4-62](#)
  - health monitoring [6-44](#)
  - high availability [11-9](#)
  - HTTP return code maps [6-37](#)
  - parameter map
    - connection [8-5](#)
    - DNS [8-24, 8-25](#)
    - generic [8-18](#)
    - HTTP [8-2](#)
    - optimization [8-11](#)
    - RTSP [8-19](#)
    - SIP [8-20](#)
    - Skinny [8-22](#)
- predictor method [5-46, 6-30](#)
- probe
  - DNS [6-48](#)
  - Echo-TCP [6-48](#)
  - Finger [6-49](#)
  - FTP [6-50](#)
  - HTTP [6-50](#)
  - HTTPS [6-52](#)
  - IMAP [6-54](#)
  - POP [6-55](#)
  - RADIUS [6-56](#)
  - RTSP [6-56](#)
  - scripted [6-57](#)
  - SIP-TCP [6-59](#)
  - SIP-UDP [6-59](#)
  - SMTP [6-60](#)
  - SNMP [6-60](#)
  - TCP [6-61](#)
  - Telnet [6-62](#)
  - UDP [6-63](#)
  - VM [6-65](#)
  - real server [6-6](#)
  - server farm [5-37, 6-19](#)
  - SNMP users [4-22](#)
  - SSL initiation [5-53](#)
  - SSL termination [5-19](#)
  - sticky group [7-12](#)
  - sticky type [5-50](#)
  - syslog [4-13](#)
  - virtual context system options [4-11](#)
  - virtual server [5-8](#)
- configuration checkpoint and rollback service
  - comparing checkpoint with running configuration [4-48](#)
  - creating configuration checkpoint [4-46](#)
  - deleting configuration checkpoint [4-47](#)
  - displaying checkpoint information [4-49](#)
  - overview [4-46](#)
  - rolling back configuration [4-48](#)
- configuration synchronization for redundancy [11-5](#)
- configuring
  - acceleration [5-57](#)
  - ACLs [4-59, 10-19](#)
    - EtherType [4-67](#)
    - extended [4-61](#)
    - object groups [4-70](#)
    - resequencing [4-66](#)
  - action lists for application acceleration [13-3](#)
  - action lists for HTTP header modify [12-90](#)
  - bandwidth optimization [5-58](#)
  - BVI interfaces [10-23](#)
  - class map match conditions
    - generic server load balancing [12-19](#)
    - Layer 7 SIP deep packet inspection [12-31](#)
    - RADIUS server load balancing [12-20](#)
    - RTSP server load balancing [12-21](#)
    - SIP server load balancing [12-23](#)
  - class maps [12-8, 12-11](#)
  - DHCP relay [10-19](#)
  - DNS probe expect address [6-66](#)

- Gigabit Ethernet interfaces [10-5](#)
- health monitoring general attributes [6-44](#)
- high availability
  - groups [11-11, 11-14](#)
  - host tracking [11-20](#)
  - interface tracking [11-19](#)
  - peer host probes [11-22](#)
  - peers [11-8](#)
  - synchronization [11-5](#)
  - tracking and failure detection [11-17](#)
- host probes for high availability [11-21](#)
- HTTP probe headers [6-66](#)
- HTTP retcode maps [6-36](#)
- HTTPS probe headers [6-66](#)
- latency optimization [5-58](#)
- Layer 7 default load balancing [5-55](#)
- load balancing
  - for server farms [6-18](#)
  - on virtual servers [5-30](#)
  - sticky groups [7-11](#)
- management VLAN [4-2](#)
- NAT [5-61, 10-32](#)
- object groups
  - ICMP service parameters [4-76](#)
  - IP addresses [4-71](#)
  - protocols [4-73](#)
  - subnet objects [4-72](#)
  - TCP/UDP service parameters [4-73](#)
- OID for SNMP probes [6-68](#)
- optimization [5-57](#)
  - action lists [5-60](#)
  - traffic policies [13-6](#)
- parameter maps
  - connection [8-5](#)
  - DNS [8-23](#)
  - generic [8-17](#)
  - HTTP [8-2](#)
  - optimization [8-11, 13-6](#)
  - RDP [8-24](#)
  - RTSP [8-19](#)
  - SIP [8-20](#)
  - Skinny [8-22](#)
- PAT [10-32](#)
- policy map rules and actions [12-36](#)
  - generic server load balancing [12-54](#)
  - HTTPS server load balancing [12-58](#)
  - Layer 3/Layer 4 management traffic policy maps [12-45](#)
  - Layer 3/Layer 4 network traffic policy maps [12-37](#)
  - Layer 7 deep packet inspection policy maps [12-73](#)
  - Layer 7 FTP command inspection policy maps [12-79](#)
  - Layer 7 HTTP optimization policy maps [12-86](#)
  - Layer 7 server load-balancing traffic policy maps [12-46](#)
  - Layer 7 SIP deep packet inspection [12-82](#)
  - Layer 7 Skinny deep packet inspection [12-84](#)
  - RADIUS server load balancing [12-63](#)
  - RDP server load balancing [12-71](#)
  - RTSP server load balancing [12-65](#)
  - SIP server load balancing [12-68](#)
- port channel interfaces [10-2](#)
- probe expect status [6-67](#)
- protocol inspection [5-20](#)
- real servers [6-11](#)
- resource classes [4-38](#)
- server farm predictor method [6-29](#)
- shared objects [5-10](#)
- SNMP [4-19](#)
  - communities [4-20](#)
  - notification [4-25](#)
  - on virtual contexts [4-19](#)
  - trap destination hosts [4-23](#)
  - users [4-21](#)
- SSL
  - chain group parameters [9-25](#)
  - CSR parameters [9-26](#)

- for virtual servers [5-18](#)
  - OCSP service [9-30](#)
  - parameter map [9-19](#)
  - parameter map cipher attributes [9-22](#)
  - proxy service [9-28](#)
- static routes [10-34](#)
- sticky groups [5-50, 7-11](#)
- sticky statics [7-21](#)
- switch mode [4-6](#)
- syslog
  - logging [4-12](#)
  - log hosts [4-16](#)
  - log messages [4-17](#)
  - log rate limits [4-18](#)
- traffic policies [12-1](#)
- virtual context [4-1, 4-2, 4-7, 4-84](#)
  - expert options [4-79](#)
  - global policies [4-28](#)
  - policy maps [12-34](#)
  - primary attributes [4-11](#)
  - system attributes [4-11](#)
- virtual server
  - configuration overview [5-2](#)
  - default Layer 7 load balancing [5-55](#)
  - Layer 7 load balancing [5-30](#)
  - NAT [5-61](#)
  - properties [5-10](#)
  - protocol inspection [5-20](#)
  - shared objects [5-9](#)
  - SSL termination service [5-18](#)
- VLAN
  - interface access control [10-18](#)
  - interface policy maps [10-18](#)
  - interfaces [10-10](#)
- connection parameter map
  - attributes [8-5](#)
  - configuring [8-5](#)
  - TCP options [8-9](#)
  - using [8-1](#)
- contact information, SNMP [4-19](#)
- context
  - archive naming convention for archive [4-50](#)
  - auto-synchronization of CLI configuration changes [4-80](#)
  - CLI synchronization state [4-80](#)
  - configuration options [4-8](#)
  - configuring [4-7](#)
    - BVI interfaces [10-23](#)
    - global policies [4-28](#)
    - load balancing [5-1](#)
    - primary attributes [4-11](#)
    - static routes [10-34](#)
    - virtual servers [5-1](#)
    - VLAN interfaces [10-10](#)
  - creating [4-2](#)
  - definition [GL-6](#)
  - deleting [4-84](#)
  - editing [4-84](#)
  - modifying [4-84](#)
  - synchronizing configurations, automatic [4-80](#)
  - synchronizing configurations, manual [4-82](#)
  - viewing all [4-84](#)
- control [10-18](#)
- controlling access to Cisco ACE appliance [15-3](#)
- conventions
  - in ACE Appliance Device Manager, table [1-12](#)
  - in this guide [iii-xix](#)
  - radio buttons, dropdown lists [4-7](#)
- cookie
  - client [7-3](#)
  - sticky client identification [7-3](#)
- copying
  - ACE licenses [4-30](#)
- CPU
  - monitoring ACE usage of [15-36](#)
- creating
  - ACLs [4-59](#)
  - diagnostic packages [16-1](#)

- domains [15-33](#)
- user accounts [15-8](#)
- user roles [15-28](#)
- virtual contexts [4-2](#)

## CSR

- configuring parameters [9-26](#)
- definition [GL-2](#)
- generating for SSL [9-27](#)

## D

### Data Center Interconnect (DCI)

- VM controller configuration [6-16](#)

### Data Encryption Standard (DES), definition [GL-2](#)

### deep packet inspection

- class maps [12-25](#)
- policy map options [12-43](#)

#### SIP

- class map match conditions [12-31](#)
- policy map rules and actions [12-82](#)

- Skinny policy map rules and actions [12-84](#)

- default user [15-5](#)

### deleting

- ACLs [4-69](#)
- active users [15-12](#)
- class map in use [12-8](#)
- domain objects [15-35](#)
- domains [15-34](#)
- files off the ACE [16-9](#)
- high availability groups [11-17](#)
- host probes for high availability [11-22](#)
- Lifeline packages [16-4](#)
- peer host probes [11-23](#)
- resource classes [4-41](#)
- role rules [15-31](#)
- SSL objects [9-2](#)
- user accounts [15-10](#)
- user roles [15-30](#)
- virtual contexts [4-84](#)

- DES, definition [GL-2](#)

### device

- using ping [14-36](#)

- device management, monitoring [15-2](#)

- DFP, definition [GL-2](#)

- DHCP relay, configuring [10-19](#)

### diagnostic tools

- file browser [16-6](#)

- disk usage, monitoring ACE [15-36](#)

### displaying

- current user sessions [15-11](#)
- list of users [15-8](#)
- network domains [15-32](#)
- user roles [15-27](#), [15-28](#)
- users who have a selected role [15-28](#)

- distinguished name, definition [GL-2](#)

### DNS

- application protocol support [12-6](#)
- configuring protocol inspection [5-20](#)
- parameter map
  - attributes [8-24](#), [8-25](#)
  - configuring [8-23](#)

### DNS probe

- attributes [6-48](#)
- expect address [6-66](#)

### document

- intended audience [iii-xv](#)
- organization [iii-xv](#)

### documentation

- obtaining [iii-xix](#)
- related [iii-xvii](#)

### domains

- attributes [15-33](#)
- creating [15-33](#)
- deleting [15-34](#)
- displaying [15-32](#)
- editing [15-34](#)
- guidelines [15-31](#)
- managing [15-31](#)



- understanding [15-7](#)
- downloading, files to ACE [16-7](#)
- Dynamic Feedback Protocol (DFP), definition [GL-2](#)
- Dynamic Workload Scaling
  - configure
    - Nexus 7000 [6-15](#)
    - overview [6-14](#)
  - server farm [5-39, 6-21](#)

---

## E

- Echo-TCP probe attributes [6-48](#)
- e-commerce
  - applications, sticky requirements [7-1](#)
  - using stickiness [7-4](#)
- editing
  - domains [15-34](#)
  - role rules [15-31](#)
  - user account info [15-10](#)
  - user roles [15-30](#)
- encryption, password [15-9](#)
- error
  - monitoring, list of polling messages [14-15](#)
- Ethernet interfaces, configuring [10-5](#)
- EtherType ACL, configuring [4-67](#)
- event, definition [GL-2](#)
- event type, definition [GL-2](#)
- exception, definition [GL-2](#)
- expert options for virtual contexts [4-79](#)
- exporting
  - SSL
    - certificates [9-16](#)
    - key pair [9-18](#)
- extended ACL
  - configuration options [4-62](#)
  - resequencing entries [4-66](#)

---

## F

- fail action
  - real server in a server farm [5-37, 6-19](#)
  - reassign [5-38, 6-20](#)
- failover [11-4](#)
- fault, definition [GL-2](#)
- fault tolerance
  - groups [11-3](#)
  - task overview [11-8](#)
- file browser
  - deleting files [16-9](#)
  - downloading files [16-7](#)
  - renaming files [16-8](#)
  - tasks [16-6](#)
  - uploading files [16-7](#)
  - viewing files [16-9](#)
- File Transfer Protocol (FTP), definition [GL-2](#)
- filtering tables [1-13](#)
- Finger probe attributes [6-49](#)
- first-match policy map [12-34](#)
- forcing logouts [15-12](#)
- FTP
  - application protocol support [12-6](#)
  - configuring protocol inspection [5-21](#)
  - definition [GL-2](#)
- FTP command inspection class map match conditions [12-30](#)
- FTP probe attributes [6-50](#)
- FTP strict, and RFP standards [12-79](#)
- FT VLAN [11-5](#)

---

## G

- gateway, default [4-3](#)
- generic parameter map
  - attributes [8-18](#)
  - configuring [8-17](#)
- generic server load balancing

- class map match conditions [12-19](#)
- policy map rules and actions [12-54](#)
- getting started
  - flowchart [1-18](#)
  - task overview [1-18](#)
- global acceleration and optimization [13-9](#)
- global policies, configuring for virtual contexts [4-28](#)
- GMT [1-16](#)
- graph
  - icons for [1-16](#)
  - maximum number of statistics [1-16](#)
  - viewing results [1-16](#)
- graphs
  - using GMT [1-16](#)
- graphs, historical trend and real time [14-31](#)
- guided setup
  - ACE hardware setup [3-3](#)
  - ACE network topology overview [3-9](#)
  - application setup [3-10](#)
  - operating considerations [3-3](#)
  - overview [3-1](#)
  - tasks and related topics [3-2](#)
  - virtual context setup [3-7](#)
- guidelines
  - Lifeline [16-2](#)
- guidelines for managing
  - domains [15-31](#)
  - user accounts [15-8](#)
  - user roles [15-14](#)

---

## H

- hash load-balancing methods
  - address [6-2](#)
  - cookie [6-2](#)
  - header [6-2](#)
  - url [6-2](#)
- header
  - insertion [12-47](#)

- rewrite [12-47](#)
- header insertion
  - configuring HTTP [12-91](#)
  - HTTP [12-92](#)
  - SSL [12-97](#)
- health monitoring
  - configuring [6-40](#)
  - for real servers [6-41](#)
  - general attributes [6-44](#)
  - inband [5-40, 6-22](#)
  - overview [6-39](#)
  - probe types [6-42](#)
  - TCL scripts [6-40](#)
- heartbeat packets [11-3](#)
- high availability
  - clearing
    - links between ACE appliances [11-11](#)
    - pairs [11-11](#)
  - configuration attributes [11-9](#)
  - configuring
    - groups [11-11](#)
    - host probes [11-21](#)
    - host tracking process [11-20](#)
    - interface tracking process [11-19](#)
    - overview [11-2](#)
    - peer host probes [11-22](#)
    - peers [11-8](#)
  - deleting
    - groups [11-17](#)
    - host probes [11-22](#)
    - peer host probes [11-23](#)
  - failover detection [11-17](#)
  - importance of synchronizing configurations [11-6](#)
  - modifying groups [11-14](#)
  - protocol [11-3](#)
  - switching over a group [11-16](#)
  - task overview [11-8](#)
  - tracking status [11-17](#)
- historical trend graph [14-31](#)

- homepage [2-1](#)
    - link descriptions [2-1](#)
    - overview [2-1](#)
    - pages in ANM [2-2](#)
  - Hot Standby Router Protocol (HSRP), definition [GL-3](#)
  - HSRP, definition [GL-3](#)
  - HTTP
    - application protocol support [12-6](#)
    - configuring
      - parameter maps [8-2](#)
      - retcode maps [6-36](#)
    - content
      - sticky group attributes [7-16](#)
      - sticky type [7-3](#)
    - cookie
      - sticky group attributes [7-17](#)
      - sticky type [7-3](#)
    - header
      - sticky client identification [7-4](#)
      - sticky group attributes [7-18](#)
      - sticky type [7-4](#)
    - parameter map attributes [8-2](#)
    - parameter maps [8-1, 8-2](#)
    - probe
      - return code map configuration options [6-37](#)
    - probe attributes [6-50](#)
  - HTTP compression, enabling [5-52, 5-56](#)
  - HTTP deep packet inspection class map match conditions [12-25](#)
  - HTTP header
    - configuring [12-91](#)
    - deletion [12-92](#)
    - insertion [12-47, 12-92](#)
    - rewrite [12-47, 12-92](#)
  - HTTP optimization action list, configuring [13-3](#)
  - HTTP optimization policy map rules [12-87](#)
  - HTTP probe, configuring headers [6-66](#)
  - HTTP protocol inspection
    - class map match conditions [12-26](#)
    - conditions and options [5-23](#)
    - policy map rules [12-74](#)
  - HTTPS probe
    - attributes [6-52](#)
    - configuring headers [6-66](#)
  - HTTPS protocol inspection conditions and options [5-23](#)
  - HTTPS server load balancing
    - policy map rules and actions [12-58](#)
- 
- ## I
- ICMP
    - application protocol support [12-6, 12-7](#)
    - definition [GL-3](#)
  - ICMP service parameters, for object groups [4-76](#)
  - icon descriptions
    - in monitor screens [1-16](#)
    - in tables [1-11](#)
  - IETF trap
    - SNMP [4-20](#)
  - ILS inspection [12-7](#)
  - IMAP probe attributes [6-54](#)
  - importing
    - ACE licenses [4-30](#)
    - SSL
      - certificates [9-8](#)
      - key pair [9-12](#)
  - inband health monitoring [5-40, 6-22](#)
    - connection failure count [5-40, 6-22](#)
    - reset timeout [5-40, 6-22](#)
    - resume service [5-41, 6-23](#)
  - installing ACE appliance licenses [4-30](#)
  - intended audience of this document [iii-xv](#)
  - interface
    - ACE Appliance Device Manager [1-6](#)
    - definition [GL-3](#)
    - Gigabit Ethernet, configuring [10-5](#)
    - Internet Control Message Protocol (ICMP), definition [GL-3](#)

IP addresses, for object groups [4-71](#)

IP netmask

for sticky client identification [7-4](#)

sticky group attributes [7-18](#)

sticky type [7-4](#)

IPv6 considerations [1-20](#)

IPv6 prefix

for sticky client identification [7-4](#)

sticky type [7-4](#)

## K

KAL-AP

configuring secure [6-70](#)

primary server farm out of service [5-15, 12-41](#)

key pair

exporting for SSL [9-18](#)

generating [9-15](#)

importing for SSL [9-12](#)

SSL [9-11](#)

## L

latency optimization, configuring [5-58](#)

Layer 3/Layer 4

management traffic

class map match conditions [12-14](#)

policy map rules and actions [12-45](#)

network traffic class maps, setting match conditions [12-11](#)

network traffic policy maps

setting rules and actions [12-37](#)

Layer 4 payload

sticky group attributes [7-19](#)

sticky type [7-4](#)

Layer 7

configuring load balancing for HTTP/HTTPS [5-30](#)

default load balancing on virtual servers [5-55](#)

FTP command inspection class maps, setting match conditions [12-30](#)

FTP command inspection policy maps, setting rules and actions [12-79](#)

HTTP deep packet inspection class maps, setting match conditions [12-25](#)

HTTP deep packet inspection policy maps, setting rules and actions [12-73](#)

HTTP optimization policy maps, setting rules and actions [12-86](#)

load balancing

rule types [5-32](#)

setting match conditions [5-31](#)

load-balancing class maps, setting match conditions [12-16](#)

load-balancing policy maps, setting rules and actions [12-46](#)

SIP deep packet inspection

class map match conditions [12-31](#)

policy map rules and actions [12-82](#)

Skinny deep packet inspection policy map rules and actions [12-84](#)

SLB policy actions

HTTP header insertion [12-47](#)

least bandwidth, load-balancing method [6-3](#)

leastconns, load-balancing method [6-3](#)

least loaded, load-balancing method [6-3](#)

license

viewing ACE license details [4-34](#)

licenses

importing [4-30](#)

installing [4-30](#)

managing for ACE appliances [4-29](#)

removing [4-33](#)

updating [4-32](#)

Lifeline

creating a package from the CLI [16-5](#)

creating a package from the DM GUI [16-3](#)

deleting packages [16-4](#)

downloading a package [16-3](#)

guidelines for use [16-2](#)

- maximum packages [16-2](#)
- load balancing
  - configuration overview [5-1](#)
  - configuring
    - for real servers [6-5](#)
    - for server farms [6-18](#)
    - on virtual servers [5-30](#)
    - real servers [6-1](#)
    - server farms [6-1](#)
    - sticky groups [7-11](#)
    - with virtual servers [5-2](#)
  - definition [GL-3](#)
  - hash address [6-2](#)
  - hash cookie [6-2](#)
  - hash header [6-2](#)
  - hash secondary cookie [6-2](#)
  - hash url [6-2](#)
  - Layer 7 [5-30](#)
  - least bandwidth [6-3](#)
  - leastconns [6-3](#)
  - least loaded [6-3](#)
  - monitoring on probes [14-27](#)
  - monitoring on real servers [14-25](#)
  - monitoring on statistics [14-28](#)
  - monitoring on virtual servers [14-23](#)
  - predictors [6-2](#)
  - response [6-3](#)
  - roundrobin [6-3](#)
- load-balancing class maps
  - Layer 7 [12-16](#)
  - setting match conditions [12-16](#)
- location, SNMP [4-19](#)
- logging
  - SIP packets syslog [8-20](#)
  - syslog levels [4-12](#)
- logging into ACE Appliance Device Manager [1-4](#)

---

## M

- Management Information Base (MIB), definition [GL-3](#)
- management VLAN, adding [4-2](#)
- managing
  - domains [15-31](#)
  - real servers [6-9](#)
  - resource classes [4-35](#)
  - user accounts [15-7](#)
  - user roles [15-14](#)
  - virtual contexts [4-79](#)
  - virtual servers [5-63](#)
- match condition
  - class map
    - generic server load balancing [12-19](#)
    - Layer 7 SIP deep packet inspection [12-31](#)
    - RADIUS server load balancing [12-20](#)
    - RTSP server load balancing [12-21](#)
    - setting for [12-10](#)
    - SIP server load balancing [12-23](#)
- match conditions
  - configuring for class maps [12-11](#)
  - for Layer 7 load balancing [5-31](#)
  - for optimization [5-59](#)
  - for optimization policy maps [12-87](#)
  - HTTP optimization [12-87](#)
  - HTTP protocol inspection [12-26, 12-74](#)
  - Layer 7 load-balancing class maps [12-16](#)
  - Layer 7 load-balancing traffic policy maps [12-48](#)
  - network management class maps [12-14](#)
- MD5, definition [GL-3](#)
- memory usage, monitoring ACE [15-36](#)
- menus, understanding [1-8](#)
- Message Digest 5 (MD5), definition [GL-3](#)
- MIB, definition [GL-3](#)
- MIME types, supported [8-25](#)
- modifying
  - domains [15-34](#)
  - high availability groups [11-14](#)

real servers [6-11](#)  
 resource classes [4-40](#)  
 user accounts [15-10](#)  
 user roles [15-30](#)  
 virtual contexts [4-84](#)

#### monitoring

buttons used in graphs [1-16](#)  
 load balancing [14-23, 14-25, 14-27](#)  
 load balancing statistics [14-28](#)  
 prerequisites [14-1](#)  
 statistics [15-35](#)  
 traffic [14-21](#)  
 viewing results, description [1-16](#)

multi-match policy map [12-34](#)

## N

### Name Address Translation

configuring [10-32](#)  
 definition [GL-3](#)  
 displaying utilization [10-33](#)

### NAT

application protocol inspection support [12-6](#)  
 configuring [10-32](#)  
 configuring on virtual servers [5-61](#)  
 definition [GL-3](#)  
 display NAT pool utilization [10-33](#)

### network management traffic

class map match conditions [12-14](#)  
 policy maps, configuring rules and actions [12-45](#)

### network object group

configuring [4-70](#)  
 IP addresses [4-71](#)  
 subnet objects [4-72](#)

network topology maps [14-34](#)

No Payload Encryption (NPE) software version [1-2](#)

## O

### object

configuring for virtual servers [5-9](#)  
 definition [GL-4](#)

### object group

configuring [4-70](#)  
 ICMP service parameters [4-76](#)  
 IP addresses [4-71](#)  
 protocols [4-73](#)  
 subnet objects [4-72](#)  
 TCP/UDP service parameters [4-73](#)

### obtaining

documentation [iii-xix](#)  
 support [iii-xix](#)

OCSP service, configuring for SSL [9-30](#)

operational states of real servers [6-12](#)

operations privileges [15-6](#)

### optimization

configuration overview [13-6](#)  
 configuring [5-57](#)  
   action lists [5-60](#)  
   globally on ACE [13-9](#)  
   match conditions [5-59](#)  
   parameter maps [8-11, 13-6](#)  
   policy map rules and actions [12-86](#)  
   traffic policies [13-6](#)  
 functionality overview [13-2](#)  
 match condition types [12-87](#)  
 match criteria [5-59](#)  
 overview [13-2](#)  
 parameter maps [8-1](#)  
 traffic policies [13-2](#)  
 typical configuration flow [13-2](#)

optimization parameter map attributes [8-11](#)

organization of this document [iii-xv](#)

### overview

ACL configuration [4-58](#)  
 admin functions [15-1](#)

- application acceleration [13-2](#)
- class map [12-2](#)
- configuration [1-18](#)
- configuration tasks [1-18](#)
- load-balancing predictors [6-2](#)
- optimization [13-2](#)
- optimization traffic policies [13-6](#)
- parameter maps [8-1](#)
- policy map [12-2](#)
- protocol inspection [12-5](#)
- real server [6-3](#)
- resource classes [4-35](#)
- server farm [6-3, 6-5](#)
- server health monitoring [6-39](#)
- SSL [9-1](#)
- stickiness [7-1](#)
- sticky table [7-11](#)
- traffic policies [12-1](#)
- using SSL keys and certificates [9-4](#)
- virtual contexts [4-2](#)

## P

- parameter expander functions [8-16](#)

- parameter map

- ACE device support [8-1](#)

- attributes

- connection [8-5](#)

- DNS [8-24, 8-25](#)

- generic [8-18](#)

- HTTP [8-2](#)

- optimization [8-11](#)

- RTSP [8-19](#)

- SIP [8-20](#)

- Skinny [8-22](#)

- configuring

- connection [8-5](#)

- DNS [8-23](#)

- for SSL [9-19](#)

- generic [8-17](#)

- HTTP [8-2](#)

- optimization [8-11, 13-6](#)

- RDP [8-24](#)

- RTSP [8-19](#)

- SIP [8-20](#)

- Skinny [8-22](#)

- SSL cipher [9-22](#)

- overview [8-1](#)

- types of [8-1](#)

- using with

- policy maps [8-1](#)

- using with Layer 3/Layer 4 policy maps [8-1, 12-5](#)

- viewing list of [8-27](#)

- parameter map redirect, configuring for SSL [9-22](#)

- parent rows, in screens and tables [1-12](#)

- password, encrypting user [15-9](#)

- passwords, changing

- account [1-6](#)

- admin [15-13](#)

- in login screen [1-6](#)

- PAT

- configuring [10-32](#)

- definition [GL-4](#)

- Payload Encryption (PE) software version [1-2](#)

- peers, high availability [11-8](#)

- PEM, definition [GL-4](#)

- ping

- definition [GL-4](#)

- testing [14-36](#)

- PKCS, definition [GL-4](#)

- policy map [12-36](#)

- all-match [12-34](#)

- associating with VLAN interface [10-18](#)

- configuring

- in virtual contexts [12-34](#)

- deep packet inspection options [12-43](#)

- first-match [12-34](#)

- Layer 3/Layer 4

- management traffic, setting rules and actions [12-45](#)
- network traffic, setting rules and actions [12-37](#)
- Layer 7
  - FTP command inspection, setting rules and actions [12-79](#)
  - HTTP deep packet inspection, setting rules and actions [12-73](#)
  - HTTP optimization, setting rules and actions [12-86](#)
- Layer 7 load-balancing traffic
  - configuring rules and actions [12-46](#)
  - match condition types [12-48](#)
- multi-match [12-34](#)
- overview [5-1](#), [6-1](#), [12-2](#), [12-4](#)
- rule and action topic reference [12-36](#)
- rules and actions
  - generic server load balancing [12-54](#)
  - HTTPS server load balancing [12-58](#)
  - Layer 7 SIP deep packet inspection [12-82](#)
  - Layer 7 Skinny deep packet inspection [12-84](#)
  - RADIUS server load balancing [12-63](#)
  - RDP server load balancing [12-71](#)
  - RTSP server load balancing [12-65](#)
  - SIP server load balancing [12-68](#)
- setting rules and actions [12-36](#)
- polling
  - enabling [15-36](#)
  - error states [14-15](#)
  - failed [14-16](#)
  - not polled error [14-16](#)
  - timed out [14-16](#)
  - unknown error [14-16](#)
- POP probe attributes [6-55](#)
- port
  - definition [GL-4](#)
  - number, configuring for probes [6-45](#)
- Port Address Translation
  - configuring [10-32](#)
  - definition [GL-4](#)
- port channel interfaces
  - attributes [10-3](#)
  - configuring [10-2](#)
- predictor
  - hash address [6-2](#)
  - hash cookie [6-2](#)
  - hash header [6-2](#)
  - hash secondary cookie [6-2](#)
  - hash url [6-2](#)
  - least bandwidth [6-3](#)
  - leastconns [6-3](#)
  - least loaded [6-3](#)
  - response [6-3](#)
  - roundrobin [6-3](#)
- predictor method
  - attributes [5-46](#), [6-30](#)
  - configuring for server farms [6-29](#)
- prerequisites, monitoring [14-1](#)
- primary attributes for virtual contexts [4-11](#)
- privileges, understanding [15-6](#)
- probe
  - attribute tables [6-47](#)
  - configuring expect status [6-67](#)
  - configuring for health monitoring [6-41](#)
  - configuring SNMP OIDs [6-68](#)
  - DNS [6-48](#)
  - Echo-TCP [6-48](#)
  - Finger [6-49](#)
  - FTP [6-50](#)
  - HTTP [6-50](#)
  - HTTPS [6-52](#)
  - IMAP [6-54](#)
  - POP [6-55](#)
  - port number [6-45](#)
  - RADIUS [6-56](#)
  - RTSP [6-56](#)
  - scripted [6-57](#)
  - scripting using TCL [6-40](#)
  - SIP-TCP [6-59](#)



- SIP-UDP [6-59](#)
  - SMTP [6-60](#)
  - SNMP [6-60](#)
  - TCP [6-61](#)
  - Telnet [6-62](#)
  - types for real server monitoring [6-42](#)
  - UDP [6-63](#)
  - VM [6-65](#)
  - process, for traffic classification [12-2](#)
  - process uptime, monitoring ACE [15-36](#)
  - protocol inspection
    - configuring for virtual servers [5-20](#)
    - configuring match criteria [5-21](#)
    - HTTP/HTTPS conditions and options [5-23](#)
    - overview [12-5](#)
    - SIP conditions and options [5-27](#)
  - protocol names and numbers [4-64](#)
  - protocols for object groups [4-73](#)
  - proxy service, configuring for SSL [9-28](#)
- 
- ## R
- RADIUS
    - probe attributes [6-56](#)
    - server load balancing
      - class map match conditions [12-20](#)
      - policy map rules and actions [12-63](#)
    - sticky group attributes [7-20](#)
    - sticky type [7-5](#)
  - RBAC, definition [GL-4](#)
  - RDP
    - parameter map
      - configuring [8-24](#)
  - RDP server load balancing policy map rules and actions [12-71](#)
  - real server
    - activating [6-10](#)
    - adding to server farm [6-26](#)
    - configuration attributes [6-6](#)
    - configuring load balancing [6-1, 6-5](#)
    - definition [GL-4](#)
    - health monitoring [6-39, 6-41](#)
    - modifying [6-11](#)
    - operational states [6-12](#)
    - overview [6-3](#)
    - suspending [6-10](#)
    - viewing all [6-12](#)
  - real time graph [14-31](#)
  - Real Time Streaming Protocol (RTSP), definition [GL-5](#)
  - redundancy
    - configuration requirements [11-6](#)
    - configuration synchronization [11-5](#)
    - definition [GL-5](#)
    - FT VLAN [11-5](#)
    - protocol [11-3](#)
    - task overview [11-8](#)
  - reloading the Device Manager GUI [16-10](#)
  - removing
    - ACE appliance licenses [4-33](#)
    - domains [15-34](#)
    - rules from roles [15-31](#)
  - renaming files on ACE [16-8](#)
  - resource
    - allocation constraints [4-36](#)
    - list of [14-18](#)
  - resource class
    - adding [4-38](#)
    - allocation constraints [4-36](#)
    - attributes [4-37](#)
    - configuring [4-38](#)
    - definition [GL-5](#)
    - deleting [4-41](#)
    - managing [4-35](#)
    - modifying [4-40](#)
    - overview [4-35](#)
    - viewing use by contexts [4-41](#)
  - resource usage, viewing [14-17](#)
  - response load-balancing method [6-3](#)

## restore

- configuring device configuration [4-55](#)
- defaults [4-52](#)
- guidelines and limitations of [4-51](#)
- overview of configuration [4-49](#)

## rewrite

- HTTP header [12-92](#)
- SSL URL [12-95](#)

## role

- definition [GL-6](#)
- deleting [15-30](#)
- editing [15-30](#)
- options [15-9](#)
- understanding [15-5](#)

## role-based access control

- containment overview [15-4](#)
- definition [GL-4](#)
- users [15-7](#)

roundrobin, load-balancing predictor [6-3](#)RSA, definition [GL-5](#)

## RTSP

- application protocol support [12-7](#)
- definition [GL-5](#)
- header
  - sticky group attributes [7-20](#)
  - sticky type [7-5](#)
- parameter map
  - attributes [8-19](#)
  - configuring [8-19](#)
- probe attributes [6-56](#)
- server load balancing
  - class map match conditions [12-21](#)
  - policy map rules and actions [12-65](#)

## rules

- changing [15-31](#)
- setting for policy maps [12-36](#)

## S

SCCP inspection [12-7](#)screens, understanding [1-8](#)

## scripted probe

- attributes [6-57](#)
- overview [6-40](#)

## secondary IP groups

- BVI interfaces [10-24](#)
- VLAN interfaces [10-18](#)

secure KAL-AP [6-70](#)security guidelines, Cisco [iii-xix](#)

## server

- activating
  - real [6-10](#)
  - virtual [5-64](#)
- managing [6-9](#)
- suspending
  - real [6-10](#)
  - virtual [5-65](#)

## server farm

- adding real servers [6-26](#)
- configuration attributes [5-37, 6-19](#)
- configuring
  - HTTP return error-code checking [6-36](#)
  - load balancing [6-1, 6-18](#)
  - predictor method [6-29](#)
- definition [GL-5](#)
- Dynamic Workload Scaling [5-39, 6-21](#)
- fail action for real server in [5-37, 6-19](#)
- fail action reassign across VLANs [5-38, 6-20](#)
- health monitoring [6-39](#)
- inband health monitoring [5-40, 6-22](#)
- overview [6-3, 6-5](#)
- predictor method attributes [5-46, 6-30](#)
- primary out of service to GSS [5-15, 12-41](#)
- sticky enabled on backup [7-15](#)
- viewing list of [6-38](#)

Server Load Balancer (SLB), definition [GL-5](#)

- server load balancing
  - generic class map match conditions [12-19](#)
  - generic policy map rules and actions [12-54](#)
  - HTTPS policy map rules and actions [12-58](#)
  - RADIUS class map match conditions [12-20](#)
  - RADIUS policy map rules and actions [12-63](#)
  - RDP policy map rules and actions [12-71](#)
  - RTSP class map match conditions [12-21](#)
  - RTSP policy map rules and actions [12-65](#)
  - SIP class map match conditions [12-23](#)
  - SIP policy map rules and actions [12-68](#)
- service, definition [GL-5](#)
- service object group
  - configuring [4-70](#)
  - ICMP service parameters [4-76](#)
  - protocols [4-73](#)
  - TCP/UDP service parameters [4-73](#)
- setup sequence for SSL [9-5](#)
- shared object
  - configuring [5-10](#)
  - configuring for virtual servers [5-9](#)
  - when deleting virtual servers [5-10](#)
- Simple Message Transfer Protocol (SMTP), definition [GL-5](#)
- SIP
  - configuring protocol inspection [5-27](#)
  - deep packet inspection
    - class map match conditions [12-31](#)
    - policy map rules and actions [12-82](#)
  - header sticky type [7-5](#)
  - logging packets in the syslog [8-20](#)
  - parameter map
    - attributes [8-20](#)
    - configuring [8-20](#)
  - protocol inspection conditions and options [5-27](#)
  - server load balancing
    - class map match conditions [12-23](#)
    - policy map rules and actions [12-68](#)
- SIP inspection [12-7](#)
- SIP-TCP probe attributes [6-59](#)
- SIP-UDP probe attributes [6-59](#)
- Skinny
  - deep packet inspection policy map rules and actions [12-84](#)
  - parameter map
    - attributes [8-22](#)
    - configuring [8-22](#)
- SLB, definition [GL-5](#)
- SMTP
  - definition [GL-5](#)
  - probe attributes [6-60](#)
- SNMP
  - configuration attributes [4-19](#)
  - configuring
    - communities [4-20](#)
    - notification [4-25](#)
    - trap destination hosts [4-23](#)
    - users [4-21](#)
  - contact information [4-19](#)
  - credentials missing [14-15](#)
  - IETF trap [4-20](#)
  - location [4-19](#)
  - probe attributes [6-60](#)
  - protocol and monitoring [14-2](#)
  - setting up for monitoring [14-2](#)
  - trap destination host configuration [4-23](#)
  - trap source interface [4-20](#)
  - unmask community [4-19](#)
  - user configuration attributes [4-22](#)
- special characters for matching string expressions [12-89](#)
- special configuration file, definition [GL-5](#)
- SSL
  - certificate
    - bulk importing attributes [9-10](#)
    - exporting attributes [9-17](#)
    - ignore authentication failure errors [9-21](#)
    - importing attributes [9-9](#)
    - overview [9-4](#)

- redirect authentication failureconfiguring
  - SSL
    - parameter map redirect attributes 9-22
    - using 9-6
- configuring
  - auth group certificates 9-32
  - chain group certificates 9-25
  - chain group parameters 9-25
  - CSR parameters 9-26
  - for virtual servers 5-18
  - OCSPPservice 9-30
  - parameter map 9-19
  - parameter map cipher attributes 9-22
  - parameter map redirect attributes 9-22
  - proxy service 9-28
- editing parameter map cipher info 9-22
- exporting
  - certificates 9-16
  - key pairs 9-18
  - keys 9-18
- generating
  - CSR 9-27
  - key pair 9-15
- header insertion, configuring 12-96
- importing
  - certificates 9-8
  - key pairs 9-12
- key pair
  - bulk importing attributes 9-14
  - exporting 9-18
  - generating 9-15
  - importing 9-12
  - importing attributes 9-13
  - overview 9-4
  - using 9-11
- load balancing on SSL cipher or cipher strength 5-34, 12-50
- objects, deleting 9-2
- overview 9-1
- parameter map cipher table 9-22
- procedure overview 9-4
- sample certificate and key pair 9-7
- setup sequence 9-5
- sticky group attributes 7-21
- URL rewrite, configuring 12-94
- SSL certificate, using 9-6
- SSL header insertion, configuring 12-96
- SSL key, using 9-11
- SSL setup sequence, using 9-5
- static route
  - configuring 10-34
  - viewing by context 10-35
- statistics
  - ACE 15-35
  - collection 14-33, 15-35
  - monitoring 15-35
  - viewing ACE 15-35
- status for the ACE appliance 15-35
- stickiness
  - cookie-based 7-3
  - HTTP content 7-3
  - HTTP cookie 7-3
  - HTTP header 7-4
  - IP netmask 7-4
  - IPv6 prefix 7-4
  - Layer 4 payload 7-4
  - overview 7-1
  - RADIUS 7-5
  - RTSP header 7-5
  - SIP header 7-5
  - sticky group 7-6
  - sticky table 7-11
  - types 7-2
- sticky
  - cookies for client identification 7-3
  - definition GL-6
  - e-commerce application requirements 7-1

- enabled on backup server farm [7-15](#)
  - groups [7-6](#)
  - HTTP header for client identification [7-4](#)
  - IP netmask for client identification [7-4](#)
  - IPv6 prefix for client identification [7-4](#)
  - overview [7-2](#)
  - table [7-11](#)
  - types [7-2](#)
  - sticky group
    - attributes
      - HTTP content [7-16](#)
      - HTTP cookie [7-17](#)
      - HTTP header [7-18](#)
      - IP netmask [7-18](#)
      - Layer 4 payload [7-19](#)
      - RADIUS [7-20](#)
      - RTSP header [7-20](#)
      - SSL [7-21](#)
    - buddy [7-6](#)
    - configuration attributes [5-50, 7-12](#)
    - configuring load balancing [7-11](#)
    - configuring sticky statics [7-21](#)
    - overview [7-6](#)
    - type-specific attributes [7-16](#)
    - viewing [7-21](#)
  - sticky statics, configuring for sticky groups [7-21](#)
  - sticky table overview [7-11](#)
  - sticky type
    - IP netmask [7-4](#)
    - HTTP content [7-3](#)
    - HTTP cookie [7-3](#)
    - HTTP header [7-4](#)
    - IPv6 prefix [7-4](#)
    - Layer 4 payload [7-4](#)
    - RADIUS [7-5](#)
    - RTSP header [7-5](#)
    - SIP header [7-5](#)
  - stopping active user sessions [15-12](#)
  - subnet objects, for object groups [4-72](#)
  - support
    - obtaining [iii-xix](#)
    - See Lifeline [16-3, 16-5](#)
  - suspend
    - definition [GL-6](#)
    - real servers [6-10](#)
    - virtual servers [5-65](#)
  - switch mode, configuring [4-6](#)
  - switchover [11-4](#)
  - synchronizing
    - all configurations [4-83](#)
    - configurations for high availability [11-6](#)
    - context configurations and high availability [4-81](#)
    - contexts created in CLI [5-2](#)
    - contexts created in CLI (automatically) [5-5](#)
    - contexts created in CLI (manually) [5-5](#)
    - individual configurations, manual [4-82](#)
    - manually synchronizing virtual servers created in CLI [4-83](#)
    - virtual context configurations [4-79](#)
  - syslog
    - configuration attributes [4-13](#)
    - configuring
      - logging [4-12](#)
      - log hosts [4-16](#)
      - log messages [4-17](#)
      - log rate limits [4-18](#)
    - logging levels [4-12](#)
- 
- ## T
- table
    - button descriptions [1-11](#)
    - conventions [1-12](#)
    - customizing [1-14](#)
    - filtering information in [1-13](#)
    - ICMP type numbers and names [4-65, 4-66, 4-77](#)
    - icon descriptions [1-11](#)

- parent rows [1-12](#)
- probe attributes [6-47](#)
- protocol names and numbers [4-64](#)
- sticky group attributes [7-16](#)
- topic reference for policy map rules and actions [12-36](#)
- takeover, forcing in high availability [11-16](#)
- task overview, redundancy [11-8](#)
- TCL script
  - health monitoring [6-40](#)
  - overview [6-40](#)
- TCP
  - definition [GL-6](#)
  - options for connection parameter maps [8-9](#)
  - probe attributes [6-61](#)
  - service parameters for object groups [4-73](#)
- Telnet probe attributes [6-62](#)
- terminating active user sessions [15-12](#)
- terminology used in ACE Appliance Device Manager [1-22](#)
- threshold, definition [GL-6](#)
- topic reference for configuring rules and actions [12-36](#)
- topology maps [14-34](#)
- traceroute, definition [GL-6](#)
- tracking user actions [14-36](#)
- traffic, monitoring [14-21](#)
- traffic class components [12-3](#)
- traffic classification process [12-2](#)
- traffic policy
  - ACE device support [12-2](#)
  - components [12-4](#)
  - configuring [12-1](#)
  - for application acceleration [13-2](#)
  - for optimization [13-2](#)
  - lookup order [12-4](#)
  - overview [12-1](#)
  - supported actions [12-2](#)
- Transfer Control Protocol (TCP), definition [GL-6](#)
- trap source interface, SNMP [4-20](#)

- troubleshooting
  - using file browser [16-6](#)
- types of users [15-5](#)

---

## U

- UDP probe attributes [6-63](#)
- UDP service parameters, for object groups [4-73](#)
- understanding
  - domains [15-7](#)
  - operations privileges [15-6](#)
  - roles [15-5](#)
- unmask community, SNMP [4-19](#)
- updating ACE appliance licenses [4-32](#)
- uploading
  - files to ACE [16-7](#)
  - virtual context configurations [4-83](#)
- URL rewrite, configuring [12-94](#)
- user roles, definition [GL-6](#)
- users
  - active session info [15-11](#)
  - adding new [15-8](#)
  - assigned [15-5](#)
  - default [15-5](#)
  - default role options [15-9](#)
  - deleting [15-10](#)
  - deleting active [15-12](#)
  - deleting roles [15-30](#)
  - forcing logoffs [15-12](#)
  - guidelines for managing [15-8](#)
  - logging in as [1-5](#)
  - overview [15-7](#)
  - types of [15-5](#)
  - understanding privileges [15-6](#)
- using
  - ACLs [4-58](#)
  - virtual contexts [4-2](#)

## V

- verifying GUI operational status [16-10](#)
- viewing
  - ACE appliance licenses [4-29](#)
  - ACLs by context [4-68](#)
  - all real servers [6-12](#)
  - all server farms [6-38](#)
  - all sticky groups [7-21](#)
  - all virtual contexts [4-84](#)
  - all virtual servers [5-65](#)
  - BVI interfaces by context [10-30](#)
  - configuration status [4-80](#)
  - files on the ACE [16-9](#)
  - license information [4-34](#)
  - network domains [15-32](#)
  - parameter maps by context [8-27](#)
  - polling states in monitoring [14-15](#)
  - resource class use on contexts [4-41](#)
  - static routes by context [10-35](#)
  - virtual servers [5-63](#)
  - virtual servers by context [5-63](#)
  - VLAN interfaces by context [10-22](#)
- virtual-address match condition attributes [12-11](#)
- virtual context
  - adding Admin user [4-6](#)
  - allocate interface VLAN [4-3](#)
  - configuration options [4-7](#)
  - configuring [4-1, 4-2](#)
    - BVI interfaces [10-23](#)
    - class map match conditions [12-10](#)
    - class maps [12-8](#)
    - expert options [4-79](#)
    - global policies [4-28](#)
    - load balancing services [5-1](#)
    - management VLAN [4-2](#)
    - policy map rules and actions [12-36](#)
    - policy maps [12-34](#)
    - primary attributes [4-11](#)
    - static routes [10-34](#)
    - system attributes [4-11](#)
    - VLAN interfaces [10-10](#)
  - creating [4-2](#)
  - definition [GL-6](#)
  - deleting [4-84](#)
  - managing [4-79](#)
  - modifying [4-84](#)
  - monitoring resource usage [14-17](#)
  - overview [4-2](#)
  - synchronizing configurations [4-79, 4-81](#)
  - using [4-2](#)
  - viewing
    - all contexts [4-84](#)
    - BVI interfaces [10-30](#)
    - configuration status [4-80](#)
    - static routes [10-35](#)
    - VLANS [10-22](#)
- Virtual Local Area Network (VLAN), definition [GL-6](#)
- virtual server
  - activating [5-64](#)
  - additional options [5-3](#)
  - advanced view properties [5-11](#)
  - and user roles [5-4](#)
  - basic view properties [5-17](#)
  - configuration
    - methods [5-5](#)
    - recommendations [5-5](#)
  - configuration subsets [5-8](#)
  - configuring [5-1, 5-2, 5-7](#)
    - default Layer 7 load balancing [5-55](#)
    - in ACE Appliance Device Manager [5-2](#)
    - in CLI [4-83, 5-2, 5-5](#)
    - Layer 7 load balancing [5-30](#)
    - NAT [5-61](#)
    - optimization [5-57](#)
    - properties [5-10](#)
    - protocol inspection [5-20](#)
    - shared objects [5-9](#)

- SSL [5-18](#)
- definition [GL-6](#)
- deleting and shared objects [5-10](#)
- managing [5-63](#)
- manually synchronizing CLI configurations [4-83](#)
- minimum configuration [5-2](#)
- RBAC permissions to create, modify, or delete [5-4, 15-27](#)
- recommendations for configuring [5-5](#)
- shared objects [5-5, 5-9](#)
- SSL initiation attributes [5-53](#)
- SSL termination attributes [5-19](#)
- suspending [5-65](#)
- viewing
  - all [5-65](#)
  - by context [5-63](#)
  - servers [5-63](#)

## VLAN

- allocating interface [4-3](#)
- attributes [10-10](#)
- configuring [10-10](#)
  - access control [10-18](#)
  - ACLs [10-19](#)
  - DHCP relay [10-19](#)
  - management VLAN [4-2](#)
  - NAT [10-32](#)
  - policy maps [10-18](#)
- definition [GL-6](#)
- FT VLAN for redundancy [11-5](#)
- interface
  - access control [10-19](#)
  - configuring [10-10](#)
  - DHCP relay [10-19](#)
  - NAT pools [10-32](#)
  - policy maps [10-18](#)
  - secondary IP groups for [10-18](#)
  - types of [10-11](#)
  - viewing [10-22](#)

## VLANs

- alias IP address, setting [1-21](#)
- VLAN Trunking Protocol (VTP), definition [GL-7](#)
- VM probe attributes [6-65](#)
- VTP, definition [GL-7](#)
- VTP domain, definition [GL-7](#)

---

## W

- Web server, definition [GL-7](#)
- weighted roundrobin. See roundrobin